FortiClient EMS - Admin Guide

Version 6.0.1

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

July 23, 2018
FortiClient EMS 6.0.1 Admin Guide
04-601-478341-20180723

TABLE OF CONTENTS

Change Log **8**

Introduction **9**

FortiClient EMS components 9

FortiClient EMS and Fortinet Endpoint Security Management 12

Documentation 12

What's New **13**

FortiClient EMS 6.0.0 13

Chromebook management merged to regular FortiClient EMS 13

Automatic quarantine from Fortinet Security Fabric 13

Automatic group assignment 13

Quarantine file management 13

Endpoint installed software inventory 13

Customize endpoint system quarantine message 14

FortiClient EMS 6.0.1 14

Enhanced FortiClient integration with FortiSandbox scanning 14

EMS REST API - Web Filter profile update 14

License expiry grace period 14

Getting Started **15**

Getting started with managing Windows, Mac, and Linux endpoints 15

Deploying FortiClient software to endpoints 15

Pushing configuration information to FortiClient 17

Relationship between FortiClient EMS, FortiGate, and FortiClient 17

Getting started with managing Chromebooks 23

Configuring FortiClient EMS for Chromebooks 23

Configuring the Google Admin console 23

Deploying profiles to Chromebooks 24

How FortiClient EMS and FortiClient work with Chromebooks 24

Installation Preparation **26**

System requirements 26

Licenses 26

FortiClient EMS 26

Component applications 27

Required services and ports 28

Management capacity 29

FortiClient Telemetry security features 30

Server readiness checklist for installation 30

Upgrading from an earlier FortiClient EMS version 31

Install preparation for managing Chromebooks 31

G Suite account 31

SSL certificates 32

Installation and Licensing **33**
Downloading the installation file 33
Installing FortiClient EMS 33
Installing FortiClient EMS using the CLI 35
Allowing remote access to FortiClient EMS and using custom port numbers 36
Customizing the SQL Server Express install directory 37
Installing FortiClient EMS to specify SQL Server Enterprise or Standard instance 37
Starting FortiClient EMS and logging in 39
Accessing FortiClient EMS remotely 39
Licensing FortiClient EMS 40
License status 42
Extending license expiries 42
Help with licensing 44
Specifying different ports 44
Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise 44
Testing the SQL server upgrade 46
Uninstalling FortiClient EMS 46
Chromebook-only Setup **48**
Google Admin Console setup 48
Logging into the Google Admin console 48
Adding the FortiClient Web Filter extension 49
Configuring the FortiClient Web Filter extension 49
Adding root certificates 50
Disabling access to Chrome developer tools 53
Disallowing incognito mode 53
Disallowing guest mode 53
Blocking Task Manager 54
Verifying the FortiClient Web Filter extension 55
Service account credentials 56
Configuring default service account credentials 56
Configuring unique service account credentials 57
GUI **63**
Banner 63
Left pane 63
Content pane 66
Dashboard **67**
Viewing the FortiClient Status 67
System Information widget 68
FortiClient Status charts and widgets 68
Viewing the Vulnerability Scan dashboard 70
Vulnerability Scan charts and widgets 70
Viewing current vulnerabilities 71
Viewing top ten vulnerabilities on endpoints 72

Viewing Chromebook Status 74
Endpoint Management 76
Windows, Mac, and Linux endpoints 76
Creating groups 76
Adding endpoints 76
Viewing endpoints 78
Managing endpoints 86
Provisioning FortiClient Android endpoints for central management 91
Google Domains 92
Adding Google domains 92
Viewing domains 92
Managing domains 95
Quarantine Management 96
Files 96
Viewing quarantined files 96
Whitelisting quarantined files 98
Whitelist 99
Viewing whitelisted files 99
Filtering whitelisted files 99
Editing file descriptions 100
Deleting files from the whitelist 100
Software Inventory 101
Applications 101
Filtering applications 102
Hosts 102
Filtering hosts 103
Endpoint Profiles 104
Configuring profiles 104
Editing the default profile 104
Configuring profiles for Windows, Mac, and Linux endpoints 104
Configuring profiles for Chromebooks 113
Viewing profiles 114
Assigning profiles 115
Assigning profiles to Windows, Mac, and Linux endpoints 115
Assigning profiles to Chromebooks 115
Managing profiles 115
Editing profiles 115
Cloning profiles 116
Syncing profile changes 116
Editing sync schedules 116
Deleting profiles 116
Profile references 117
Profile Name 117
AntiVirus Protection 117

Sandbox Detection 122
Web Filter 123
Application Firewall 127
VPN 128
Vulnerability Scan 133
System Settings 134
XML Configuration 140

Profile Components 141

Managing installers 141
FortiGuard Distribution Network 141
Adding FortiClient installers 141
Uploading custom FortiClient installers 143
Viewing installers 145
Deleting FortiClient installers 145
Managing FortiSandbox units 146
Adding a FortiSandbox 146
Editing a FortiSandbox 147
Viewing FortiSandboxes 147
Deleting a FortiSandbox 148
Managing CA certificates 148
Uploading certificates 148
Importing certificates 148

Gateway Lists 150

Creating gateway lists 150
Exporting gateway lists to XML 151
Viewing gateway lists 152
Assigning gateway lists to endpoints 152
Viewing assigned gateway lists 152

Deployment 153

Preparing the AD server for deployment 153
Configuring a group policy on the AD server 153
Configuring required Windows services 154
Creating deployment rules for Windows firewall 154
Configuring Windows firewall domain profile settings 154
Preparing Windows endpoints for FortiClient deployment 155
Deploying FortiClient on endpoints 155
Deploying initial installations of FortiClient (macOS) 156
Deploying FortiClient upgrades from EMS 156

Administration 158

Administrators 158
Default user account and permissions 158
Viewing users 158
Configuring Administrators 158

Administrators reference ... 159
Configuring User Server ... 161
Configuring User Settings ... 162
Group assignment rules ... 162
Tag group assignment rules ... 162
IP address group assignment rules ... 163
Group assignment rule priority levels ... 163
Adding a tag group assignment rule ... 163
Adding an IP address group assignment rule ... 164
Enabling/disabling a group assignment rule ... 164
Deleting a group assignment rule ... 164
Database management ... 165
Backing up the database ... 165
Restoring the database ... 165
License upgrades or renewals ... 165
Logs ... 166
Viewing logs ... 166
Downloading logs ... 166
System Settings ... 167
Configuring Server settings ... 167
Adding SSL certificates to FortiClient EMS ... 170
Configuring Logs settings ... 171
Configuring FortiGuard settings ... 172
Configuring Endpoints settings ... 172
Configuring the login banner ... 173
Alerts ... 173
Configuring EMS Alerts ... 173
Configuring Endpoints Alerts ... 175
Configuring SMTP Server settings ... 175
Viewing Alerts ... 177
Customizing the endpoint quarantine message ... 177
Creating a Support Package ... 179

Change Log

Date	Change Description
2018-07-23	Initial release.

Introduction

FortiClient Enterprise Management Server (FortiClient EMS) is a security management solution that enables scalable and centralized management of multiple endpoints (computers). FortiClient EMS provides efficient and effective administration of endpoints running FortiClient. It provides visibility across the network to securely share information and assign security profiles to endpoints. It is designed to maximize operational efficiency and includes automated capabilities for device management and troubleshooting. FortiClient EMS also works with the FortiClient Web Filter extension to provide web filtering for Google Chromebook users.

FortiClient EMS is designed to meet the needs of small to large enterprises that deploy FortiClient on endpoints and/or provide web filtering for Google Chromebook users. Benefits of deploying FortiClient EMS include:

- Remotely deploying FortiClient software to Windows PCs
- Updating profiles for endpoint users regardless of access location
- Administering FortiClient endpoint connections, such as accepting, disconnecting, and blocking connections
- Managing and monitoring endpoints, such as status, system, and signature information
- Identifying outdated versions of FortiClient software
- Defining web filtering rules in a profile and remotely deploying the profile to the FortiClient Web Filter extension on Google Chromebook endpoints

You can manage endpoint security for Windows and macOS platforms using a unified organizational security policy. An organizational security policy provides a full, understandable view of the security policies defined in the organization. You can see all policy rules, assignments, and exceptions in a single unified view.

FortiClient EMS components

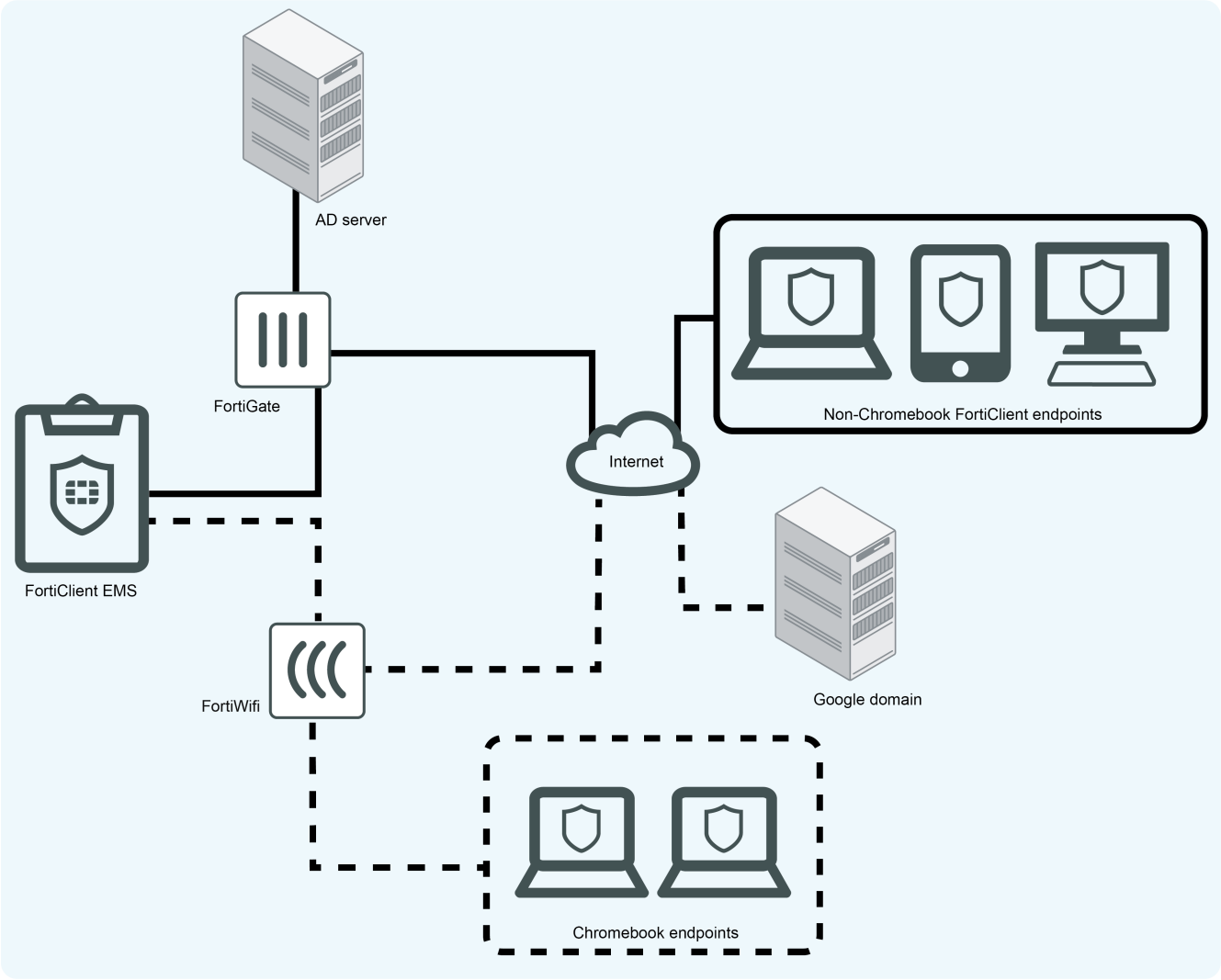
FortiClient EMS provides the infrastructure to install and manage FortiClient software on endpoints. FortiClient protects endpoints from viruses, threats, and risks.

FortiClient EMS also provides the infrastructure to install and manage the FortiClient Web Filter extension on Google Chromebook endpoints. FortiClient protects endpoint users by working with FortiClient EMS to filter web content endpoint users view on Google Chromebooks.

The following table lists FortiClient EMS components.

Component	Description
FortiClient EMS	Manages FortiClient on endpoints that connect to your network. Manages the FortiClient Web Filter extension installed on Google Chromebook endpoints, which are connected to your Google domain. Includes the following software: • Console software that manages security profiles, FortiClient on endpoints, and Chromebook endpoints • Server software that provides secure communication between endpoints and the console and between Chromebook endpoints and the Google Admin console.
Database	Stores security profiles and events. Also stores user information retrieved from the Google Admin console for Chromebooks. The SQL database is installed as part of the FortiClient EMS installation.
FortiClient	Helps enforce security and protection on endpoints. It runs on servers, desktops, and portable computers you want to secure. See the *FortiClient Administration Guide* on docs.fortinet.com/forticlient/admin-guides for information.
FortiClient Web Filter Extension	Communicates with FortiClient EMS and enforces web filtering on Google Chromebook endpoints.

In the diagram below, the undotted lines shows how different components are connected to manage Windows, Mac, and Linux endpoints using FortiClient EMS. The dotted lines represent how components are used to manage Chromebook endpoints with FortiClient EMS.



FortiClient EMS allows you to:

- Establish and enforce security profiles
- Manage deployment, configuration, and updates
- Manage security profiles from an integrated management console
- Obtain a consolidated view of multiple security components across all endpoints in your network and Google domain
- Perform integrated installation of security components and set profiles
- Monitor endpoints' web browsing activity

An informative video introducing you to FortiClient EMS is available in the Fortinet Video Library.

FortiClient EMS and Fortinet Endpoint Security Management

FortiClient EMS is part of the Fortinet Endpoint Security Management suite, which ensures comprehensive policy administration and enforcement for an enterprise network.

Documentation

You can access FortiClient EMS documentation from the following link: docs.fortinet.com/ems/admin-guides

The FortiClient EMS documentation set includes the following:

- *FortiClient EMS 6.0.1 Release Notes*

  This document describes new features and enhancements in FortiClient EMS for the release and lists any known issues and limitations. This document also defines supported platforms and minimum system requirements.
- *FortiClient EMS 6.0.1 QuickStart Guide*

  This document describes how to install and begin working with the FortiClient EMS system. It provides instructions on installation and deployment, and includes a high-level task flow for using the FortiClient EMS system.
- *FortiClient EMS 6.0.1 Administration Guide*

  This document describes how to set up FortiClient EMS and use it to manage endpoints. It includes information on how to configure multiple endpoints, configure and manage profiles for the endpoints, and view and monitor endpoints.
- *FortiClient EMS Upgrade Paths*

  This document provides upgrade path information for different versions of FortiClient EMS.

What's New

The following is a list of new features and enhancements in FortiClient EMS 6.0.

FortiClient EMS 6.0.0

Chromebook management merged to regular FortiClient EMS

You can now use a single FortiClient EMS console to manage all FortiClient platforms, including Chromebooks. All FortiClient endpoints can be managed from a single FortiClient EMS installation. Previously, a separate FortiClient EMS for Chromebooks install was needed to manage Chromebook clients. See Configuring Server settings on page 167.

Automatic quarantine from Fortinet Security Fabric

FortiClient EMS 6.0.0 supports automatic quarantine of suspicious FortiClient endpoints from the Security Fabric. An automated rule can be defined in FortiOS 6.0 to quarantine suspicious (IOC) FortiClient endpoints.

Automatic group assignment

Automatic group assignment allows you to dynamically group endpoints based on installer tags. Instead of manually creating or moving endpoints to custom groups, you can create rules which allow FortiClient EMS to automatically create dynamic groups and move endpoints to preassigned groups. See Group assignment rules on page 162.

Quarantine file management

FortiClient EMS 6.0.0 introduces central quarantine management, which shows a central view of all file-based threats detected and quarantined by FortiClient. You can restore and whitelist a quarantined file on endpoints with a single click in the case of false-positive detections. This feature requires FortiClient 6.0.0 or later versions. See Quarantine Management on page 96.

Endpoint installed software inventory

FortiClient EMS 6.0.0 introduces the Software Inventory management feature where administrators can centrally track software usage for all managed endpoints. The Software Inventory dashboard includes the name, publisher, and version of software installed on all managed endpoints. See Software Inventory on page 101.

Customize endpoint system quarantine message

You can now customize the quarantine message displayed on a user's FortiClient Console. This feature requires FortiClient 6.0.0 or later versions. See Customizing the endpoint quarantine message on page 177.

FortiClient EMS 6.0.1

Enhanced FortiClient integration with FortiSandbox scanning

EMS retrieves the list of file types from FortiSandbox. The EMS administrator may create endpoint profiles with predefined or custom lists of file types, and assign the same to endpoint groups.

Through EMS, FortiClient is able to receive a list of valid file types to monitor locally. New files introduced into the local file system with matching file types are sent to the FortiSandbox.

This feature requires FortiClient (Windows) 6.0.1 and FortiSandbox 3.0.0. See Managing FortiSandbox units on page 146.

EMS REST API - Web Filter profile update

The EMS administrator may import endpoint profiles from FortiManager. The existing feature to import endpoint profiles from FortiGate has been improved. See Importing FortiClient profiles from FortiManager on page 109.

License expiry grace period

When the license expires, the number of supported FortiClient instances remains unchanged for a few days. This allows the EMS administrator some time to download a renewal license from FortiCare and upload it to EMS.

During this grace period, the EMS GUI displays the license status as Expired, along with a link to upload a renewal license. The GUI shows the number of seats available as 10.

After the grace period is over, the number of supported FortiClient instances goes back to 10 and the license status changes to Trial, unless (and until) the renewal license is uploaded.

Getting Started

This section provides information on getting started with managing Windows, Mac, and Linux endpoints and managing Chromebooks:

Getting started with managing Windows, Mac, and Linux endpoints

This section provides an overview of how to perform the following tasks after you install and license FortiClient EMS:

- Deploying FortiClient software to endpoints on page 15
- Pushing configuration information to FortiClient on page 17
- Relationship between FortiClient EMS, FortiGate, and FortiClient on page 17

Deploying FortiClient software to endpoints

Following is an overview of how to add endpoints to FortiClient EMS and configure FortiClient EMS to deploy FortiClient to endpoints.

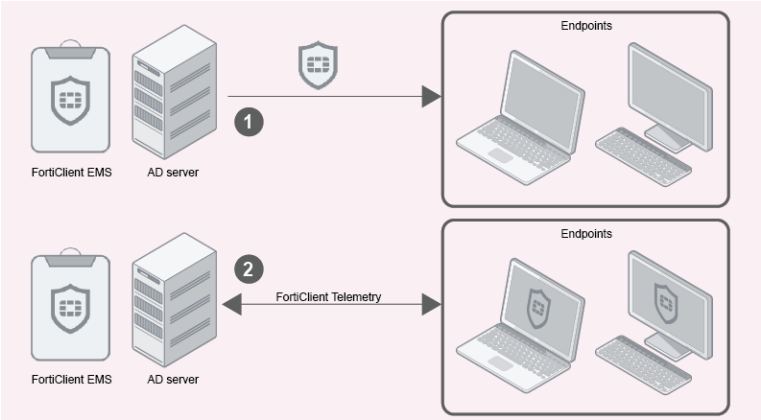
You can deploy FortiClient to endpoints using AD servers and workgroups. There are differences between using AD servers and workgroups.

When using an AD server, you can deploy an initial installation of FortiClient (Windows) to endpoints, but you cannot deploy an initial installation of FortiClient (macOS). After FortiClient for Windows or macOS is installed on endpoints and endpoints are connected to FortiClient EMS, you can deploy upgrades, uninstallations, and replacements of both FortiClient for Windows and macOS using AD servers.

When using workgroups, you cannot deploy an initial installation of FortiClient to endpoints. However, after FortiClient is installed on endpoints and endpoints are connected to FortiClient EMS, you can use workgroups to uninstall and update FortiClient on endpoints.

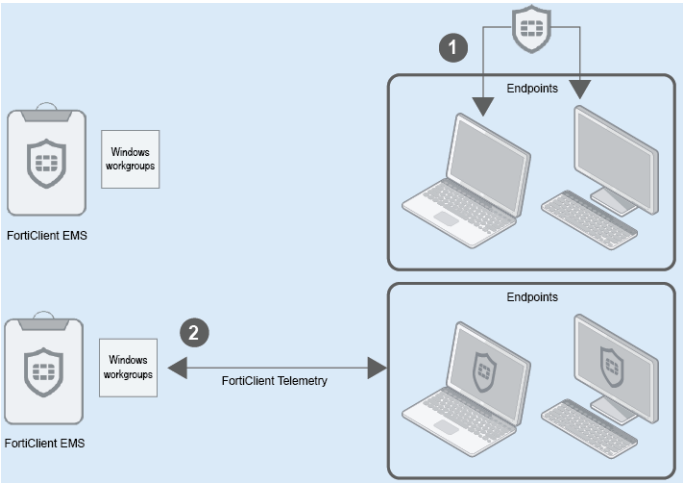
The image below shows a deployment of FortiClient using FortiClient EMS with an AD server:

1. Deploy FortiClient from FortiClient EMS using an AD server to the desired endpoints.
2. The endpoints now have FortiClient installed and FortiClient Telemetry is connected to FortiClient EMS.



The image below shows a deployment of FortiClient (Windows) using FortiClient EMS with Windows workgroups:

1. Workgroups cannot be used with FortiClient EMS to initially install FortiClient on endpoints. FortiClient must be installed directly on endpoints. Endpoint users can access *Manage Installers* in FortiClient EMS to download and install FortiClient on endpoints. See Viewing installers on page 145.
2. The endpoints now have FortiClient installed and FortiClient Telemetry is connected to FortiClient EMS.



To deploy FortiClient software to endpoints:

1. Add endpoint with an AD server or Windows workgroups. See Adding endpoints on page 76.

   Endpoints added using an AD service are displayed on the *Endpoints* > *Domains* pane, and endpoints added using Windows workgroups are displayed on the *Endpoints* > *Workgroups* pane. You can install, upgrade, and uninstall FortiClient on endpoints using an AD server without connecting FortiClient to FortiClient EMS as long as the username and password are correct on the profile's *Deployment* tab in FortiClient EMS. Note workgroups can only be used to upgrade or uninstall FortiClient if it is already installed on the endpoints and connected to FortiClient EMS; workgroups cannot be used for initial installations of FortiClient. When using workgroups, the credentials on the *Deployment* tab in FortiClient EMS are not taken into account.
2. Add FortiClient installers to FortiClient EMS, and specify which FortiClient features each installer will install on endpoints. See Adding FortiClient installers on page 141.
3. Create a profile to select the FortiClient installer and include configuration information for FortiClient software on endpoints. See Creating profiles to deploy FortiClient on page 105.
4. Prepare domains and workgroups for deployment. See Preparing the AD server for deployment on page 153.

5. Assign profiles to domains and workgroups to deploy FortiClient on endpoints. See Assigning profiles on page 115.

   See Deploying FortiClient on endpoints on page 155.

   After the profile is assigned to endpoints, its changes are pushed to endpoints. FortiClient is installed on endpoints, and FortiClient connects Telemetry to FortiClient EMS.
6. Monitor the installation process using the *Endpoints* content pane. See Viewing the Endpoints content pane on page 78.

Pushing configuration information to FortiClient

After the endpoints' FortiClient connects FortiClient Telemetry to FortiClient EMS, the endpoints are managed, and you can use FortiClient EMS to push configuration information to FortiClient software on endpoints.

To push configuration information to FortiClient:

1. Edit an existing profile or create a new profile to configure FortiClient software on endpoints. See Creating profiles to configure FortiClient on page 105.
2. Assign profiles to domains and workgroups to deploy FortiClient on endpoints. See Assigning profiles on page 115.

   After the profile is assigned to endpoints, its changes are pushed to endpoints with the next Telemetry communication.
3. Monitor the update using the *Endpoints* content pane. See Viewing the Endpoints content pane on page 78.

Relationship between FortiClient EMS, FortiGate, and FortiClient

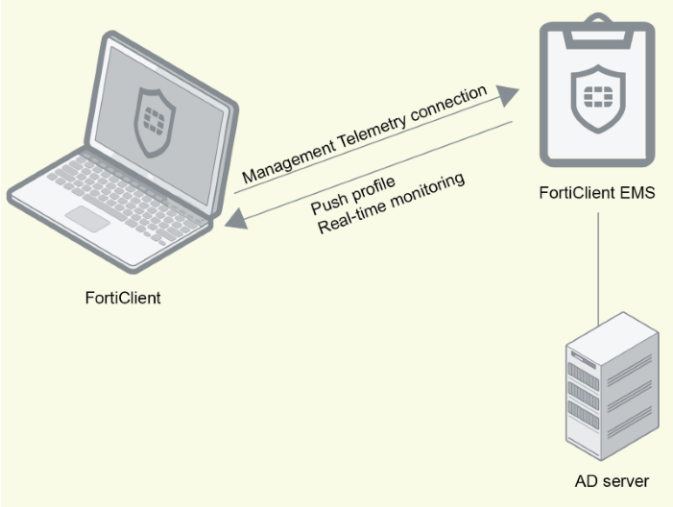
FortiClient EMS can be used in standalone mode or integrated with FortiGate. The following section illustrates the topology for each configuration and the GUI differences between the scenarios. The following table clarifies the terminology used:

Term	Definition
Fabric Telemetry connection	Connection between FortiClient and FortiOS when FortiClient is used with FortiGate.
Management Telemetry connection	Connection between FortiClient and EMS when FortiClient is used with EMS.

For details, see the *FortiClient Compliance Guide*.

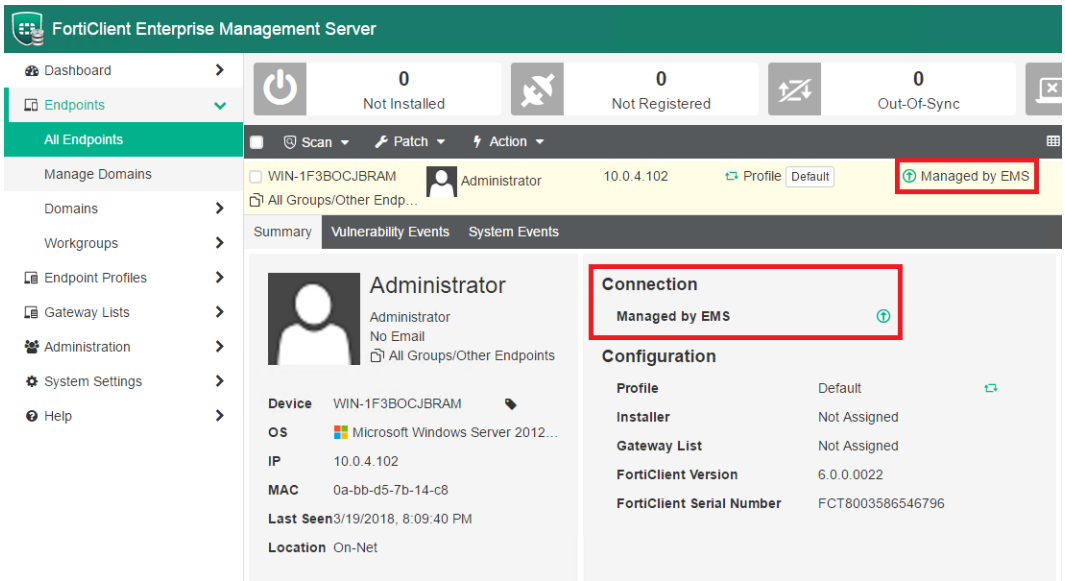
Standalone FortiClient EMS

The diagram below shows the topology when using FortiClient EMS in standalone mode.

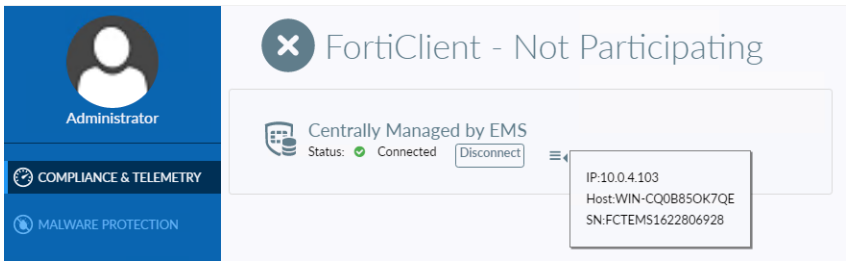


In this scenario, FortiClient EMS provides FortiClient endpoint provisioning. FortiClient endpoints connect FortiClient Telemetry to FortiClient EMS to receive configuration information from FortiClient EMS. This scenario does not support compliance.

When viewing the endpoint in the FortiClient EMS GUI, the endpoint's connection is shown as *Managed by EMS*.

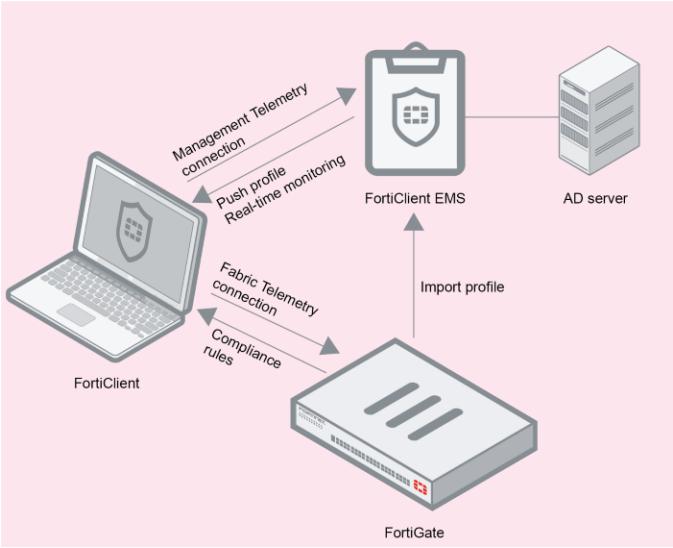


The below shows the FortiClient GUI when FortiClient is connected to FortiClient EMS but not FortiGate. FortiClient Console indicates that FortiClient is not participating in compliance enforcement because it is not connected to a FortiGate. You can also view the IP address, host name, and serial number of the EMS to which FortiClient Telemetry is connected. This means FortiClient EMS can push profiles to FortiClient. FortiClient EMS is providing endpoint provisioning to FortiClient.



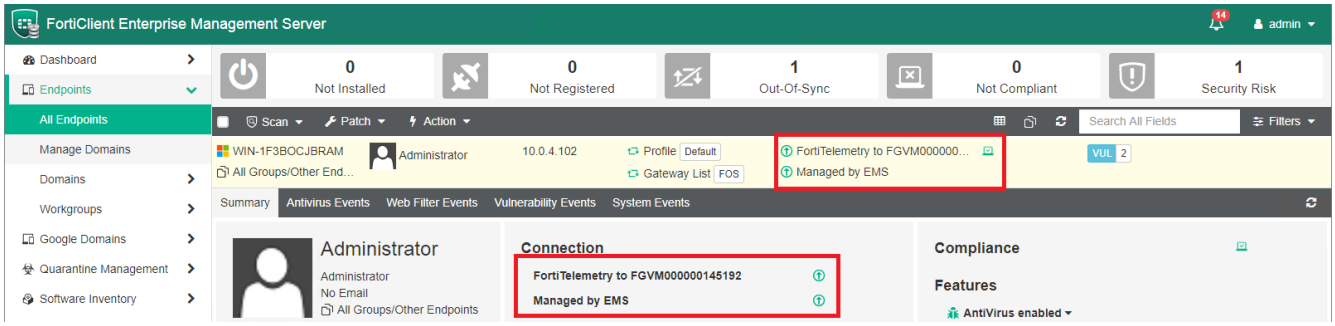
FortiClient EMS integrated with FortiGate

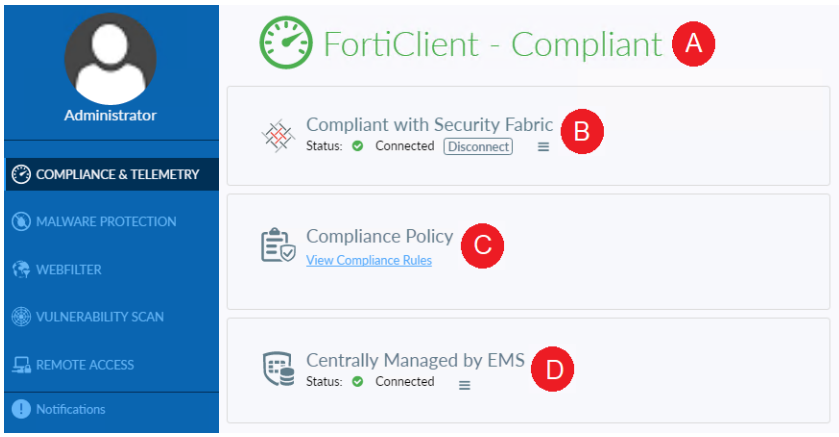
The diagram below shows the topology when using FortiClient EMS integrated with FortiGate.



In this scenario, FortiClient EMS provides FortiClient endpoint provisioning, while the FortiGate provides compliance rules to the endpoint. FortiClient endpoints connect FortiClient Telemetry to FortiClient EMS to receive configuration information from FortiClient EMS and receive compliance rules from the FortiGate. Profiles can also be imported from the FortiGate to FortiClient EMS, then pushed to the endpoints. Also see Using EMS integrated with FortiGate on page 21.

When viewing the endpoint in the FortiClient EMS GUI, the endpoint's connection is shown as *FortiTelemetry to FGT<number>* and *Managed by EMS*.





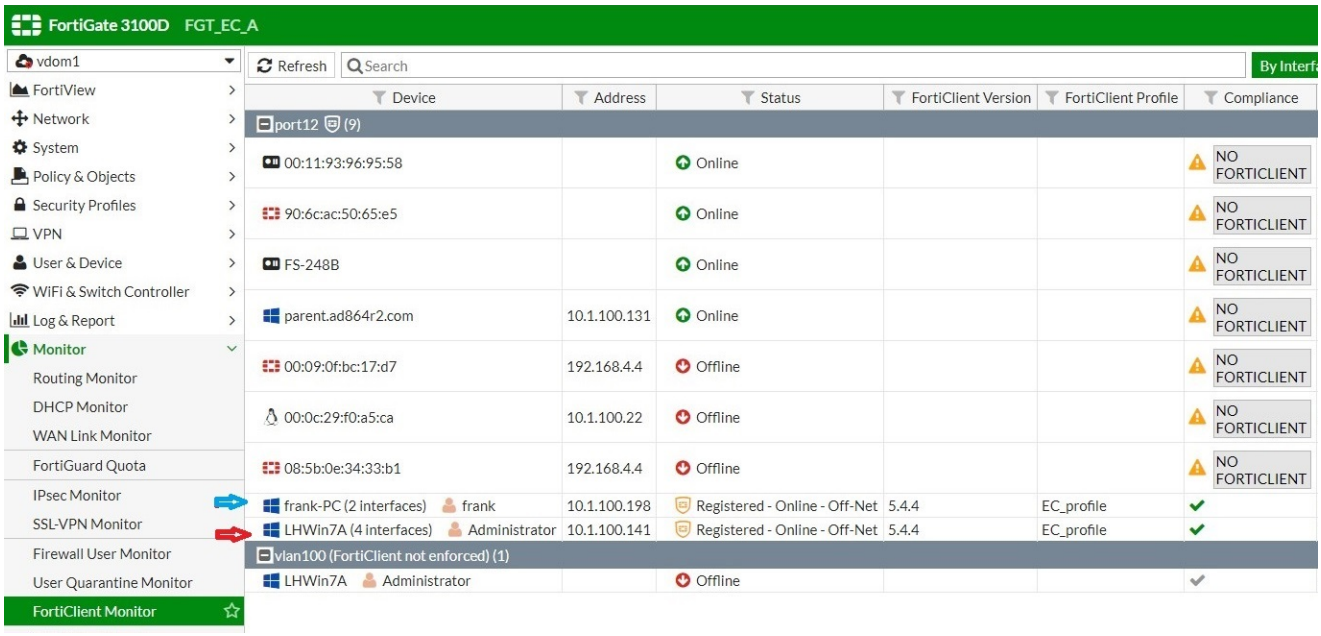
Label	Description
A	This shows the endpoint is connected to the specified FortiGate and is compliant to security policy rules defined under FortiClient Compliance profiles on that FortiGate.
B	This shows the endpoint is connected to and receiving compliance rules from the specified FortiGate. Click the menu icon to view the FortiGate's IP address, hostname, and serial number.
C	When FortiClient Telemetry is connected to FortiGate, you can view the compliance rules from FortiGate. The compliance rules communicate the configuration required for FortiClient Console and the endpoint to remain compliant. When the endpoint has a non-compliant status, an exclamation mark indicates which compliance rules are not met. See below for an example of the FortiClient Console GUI when the endpoint is not compliant.
D	View the FortiClient EMS server's name. This indicates FortiClient EMS is managing and provisioning configuration to the endpoint. Click the menu icon to view the FortiClient EMS server's IP address, hostname, and serial number.

The below shows an example of the FortiClient Console when the endpoint is not compliant with FortiGate compliance rules and may be blocked from accessing the network.

You have some time to fix the non-compliant issues before FortiGate blocks network access. When an endpoint has a non-compliant (blocked) status, you can identify which compliance rules are causing the non-compliant status under *Compliance Policy* as seen above.

You can fix non-compliant settings by clicking *Fix Non-compliant Settings*. For details, see the *FortiClient Administration Guide*.

The image below shows the FortiOS GUI. In this situation, frank-PC and LHWin7A represent two endpoints connected to the FortiGate. frank-PC is also managed by FortiClient EMS. There is no flag to identify between the scenarios.



Using EMS integrated with FortiGate

You can integrate FortiGate with FortiClient EMS. When used together, FortiGate is used for endpoint control and network access compliance (NAC), and FortiClient EMS is used to deploy and manage FortiClient software on endpoints.

When FortiGate is configured for NAC, you can use FortiOS to create a FortiClient Compliance profile that defines compliance rules and non-compliance action. The compliance rules define what configuration FortiClient software and the endpoint must have for the endpoint to maintain access to the network through FortiGate.

FortiOS 6.0.0 and later versions use one of the following two methods to determine endpoint compliance. The FortiOS configuration determines which method is used. FortiOS versions prior to 6.0.0 only use the second method below to determine endpoint compliance. In both cases, FortiClient must be installed on the endpoint.

1. An endpoint is considered compliant if FortiClient is managed by the EMS server authorized in FortiOS.
2. An endpoint is considered compliant if it complies with the specific compliance rules configured in FortiOS.

The non-compliance action can be *block* or *warn* and defines what action FortiGate takes when endpoints fail to comply with the compliance rules. When the non-compliance action is *block*, FortiGate blocks endpoints from accessing the network when they fail to comply with the compliance rules. When the non-compliance action is *warn*, FortiGate warns the endpoint about non-compliance but allows network access after the endpoint user acknowledges the warning.

Although the compliance rules define what configuration FortiClient software and the endpoint must have, the FortiClient Compliance profile from FortiGate does not include any configuration information. The endpoint user or administrator is responsible for configuring FortiClient Console to adhere to the compliance rules. An administrator can use FortiClient EMS to configure FortiClient Console.

After you create a FortiClient Compliance profile using FortiOS, you can import the profile into FortiClient EMS and edit the profile to add a FortiClient installer and specify configuration information for FortiClient software. Then you can use FortiClient EMS to deploy the updated profile containing compliance rules and configuration information to endpoints.

To use EMS integrated with FortiGate:

1. Using FortiGate running FortiOS 5.6 or a later version, define the compliance rules. Do one of the following:
   a. Configure FortiGate to consider an endpoint compliant if it has FortiClient installed and is reporting to a specified EMS server. Enter the desired FortiClient EMS server IP address or hostname. This option is only available for FortiOS 6.0.0 and later versions. If using this option, proceed to step 4.
   b. Define specific endpoint compliance rules.
2. Using FortiClient EMS, import the FortiClient Compliance profile. See Importing FortiGate profiles on page 107.
3. Review the compliance rules.
4. Do one of the following:
   a. If you configured FortiGate to consider an endpoint compliant if its FortiClient is reporting to the specified EMS server, edit your endpoint profile as desired, then save. Add a FortiClient installer if needed.
   b. If importing a FortiGate profile, edit the imported profile to add configuration information that supports the compliance rules, and save the profile. You can add a FortiClient installer if needed.
5. Create a gateway list that includes the gateway IP address or fully qualified domain name (FQDN) for the FortiGate. See Creating gateway lists on page 150.

   Each gateway list includes a list of one or more IP addresses or fully qualified domain names (FQDN) that FortiClient can use when connecting to EMS or FortiGate.
6. Assign the gateway list to domains or workgroups as needed. See Assigning gateway lists to endpoints on page 152.

   FortiClient software uses the IP addresses in the gateway list to connect FortiClient Telemetry to EMS and/or FortiGate.
7. Assign the profile to domains or workgroups as needed. See Assigning profiles on page 115.

   After the profile is assigned to endpoints, the settings are pushed to endpoints with the next Telemetry communication.
8. Use FortiClient EMS to monitor and manage endpoints. See Viewing the Endpoints content pane on page 78.
9. Use FortiClient EMS to update the profile as needed.

Quarantining an endpoint from FortiOS using EMS

In FortiOS 6.0, an administrator can quarantine FortiClient endpoints using EMS by enabling the *Quarantine FortiClient via EMS* option. The following lists the requirements for this feature:

- The FortiClient endpoint is connected to FortiGate and managed by EMS
- The FortiClient endpoint and FortiGate use the same FortiAnalyzer
- The EMS server managing the FortiClient endpoint is configured on the FortiGate. FortiOS allows configuration of up to three EMS servers to allow endpoint control in different locations.

Configuring *Quarantine FortiClient via EMS* requires using the FortiOS CLI to set the following fields: `automation-stitch` and `forticlient-ems`. See the *FortiOS CLI Reference*.

If *Quarantine FortiClient via EMS* is enabled, the following occurs when an indicator of compromise (IOC) is detected on an endpoint in the Security Fabric:

1. An IOC is detected on an endpoint.
2. FortiOS sends the endpoint information to EMS with instructions to quarantine the endpoint.
3. EMS identifies and quarantines the endpoint based on the request from FortiOS.

You can remove the endpoint from quarantine using EMS as described in Quarantining endpoints on page 89 or using FortiOS by following the procedure described below:

1. The administrator identifies that EMS has quarantined an endpoint from one of the following:
   a. FortiClient on the endpoint
   b. *Quarantine Management* or *FortiClient Monitor* in FortiOS
   c. *Endpoints* pane in EMS
2. The administrator removes the endpoint from quarantine in FortiOS.
3. FortiOS sends the endpoint information to EMS with instructions to remove the endpoint from quarantine.
4. EMS identifies and removes the endpoint from quarantine based on the request from FortiOS.

Getting started with managing Chromebooks

The following tasks are specific to Chromebook management.

This section also includes a description of how FortiClient EMS and FortiClient work with Google Chromebooks after setup is complete.

Configuring FortiClient EMS for Chromebooks

To configure FortiClient EMS for Chromebooks:

1. Start and log into FortiClient EMS. See Starting FortiClient EMS and logging in on page 39.
2. Add SSL certificates. See Adding SSL certificates to FortiClient EMS on page 170.
3. Configure FortiClient EMS settings. See System Settings on page 167.
4. Configure user accounts and permissions. See Administrators on page 158.

Configuring the Google Admin console

Following is an overview of how to configure the Google Admin console to prepare for adding the Google domain to FortiClient EMS. The document assumes you have created the Google domain.

To configure the Google Admin console:

1. Add the FortiClient Web Filter extension. See Adding the FortiClient Web Filter extension on page 49.
2. Configure the FortiClient Web Filter extension. See Configuring the FortiClient Web Filter extension on page 49.
3. Add root certificates. See Adding root certificates on page 50.
4. Configure unique service account credentials. See Configuring unique service account credentials on page 57.
5. Disallow incognito mode. See Disallowing incognito mode on page 53.

Deploying profiles to Chromebooks

Following is an overview of how to add a Google domain, configure profiles, and push profiles to Google Chromebooks. After you add the extension in the Google Admin console, the extension is downloaded to the Google Chromebook when the Chromebook user logs into the Chromebook.

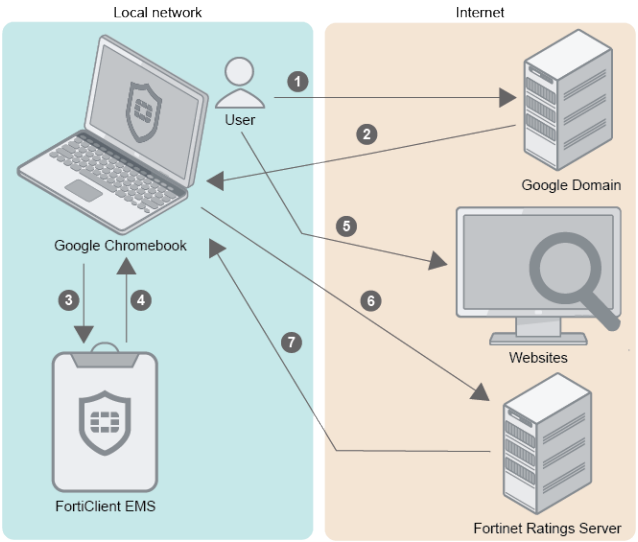
To deploy profiles to Chromebooks:

1. Add the Google domain. See Adding Google domains on page 92.
2. Define web filtering options in one or more profiles. See Adding new profiles on page 113.
   You can enable Safe Search in profiles.
3. Assign profiles to domains to deploy profiles to the FortiClient Web Filter extension on Chromebook endpoints. See Assigning profiles on page 115.
4. Verify the FortiClient Web Filter extension. See Verifying the FortiClient Web Filter extension on page 55.
5. View Google domains and Google users. See Viewing domains on page 92.

How FortiClient EMS and FortiClient work with Chromebooks

After you install and configure FortiClient EMS, the Google Admin console, and the FortiClient Web Filter extension, the products work together to provide web filtering security for Google Chromebook users logged into the Google domain. Following is a summary of how the products work together after setup is complete:

1. A user logs into the Google Chromebook.
2. The Google Chromebook downloads the FortiClient Web Filter extension.
3. FortiClient connects to FortiClient EMS.
4. FortiClient downloads a profile to the Google Chromebook. The profile contains web filtering settings from FortiClient EMS.
5. The user browses the Internet on the Google Chromebook.
6. FortiClient sends the URL query to the Fortinet Ratings Server.
7. The Fortinet Ratings Server returns the category result to FortiClient. FortiClient compares the category result with the profile to determine whether to allow the Google Chromebook user to access the URL.


Local network
Internet
User
Google Chromebook
FortiClient EMS
Google Domain
Websites
Fortinet Ratings Server
1
2
3
4
5
6
7

Installation Preparation

This section helps you prepare to install FortiClient EMS. Before installing FortiClient EMS, be aware of the following information.

Before installing FortiClient EMS, it is recommended you read the *FortiClient EMS Release Notes* available on http://docs.fortinet.com/ems/release-information to become familiar with relevant software components and other important information about the product.

System requirements

The minimum system requirements for FortiClient EMS are as follows.

- Microsoft Windows Server 2008 R2 or newer
- 2.0 GHz 64-bit processor, dual core (or two virtual CPUs)
- 4 GB RAM (8 GB RAM or more is recommended)
- 40 GB free hard disk
- Gigabit (10/100/1000baseT) Ethernet adapter
- Internet access

Internet access is required during installation. This becomes optional once installation is complete. FortiClient EMS accesses the Internet to obtain information about FortiGuard engine and signature updates.

You should only install FortiClient EMS and the default services for the operating system on the server. You should not install additional services on the same server as FortiClient EMS.

Licenses

This section describes licensing options available for FortiClient EMS. It provides information about the number of supported FortiClient endpoints and Google Chromebooks for each type of license to help determine which license best suits your needs. Note that there are separate licenses for FortiClient EMS and for FortiClient EMS for managing Google Chromebooks.

FortiClient EMS

FortiClient EMS supports the following types of licenses:

- Free trial license on page 27
- Purchased license on page 27

Free trial license

When you install FortiClient EMS, the free trial license is enabled by default. There are separate licenses for Windows/Mac/Linux endpoint management and Chromebook management.

The free trial license for Windows/Mac/Linux FortiClient EMS supports ten FortiClient endpoints. FortiClient EMS consumes one license count for each managed FortiClient device.

The free trial license for Chromebook management supports ten Google Chromebook users. FortiClient EMS consumes one license count for each logged-in user. If the user logs out, the license seat times out (default timeout being 24 hours), and the license is released. At this point, another user can use this license seat.

Purchased license

There are separate purchasable licenses for Windows/Mac/Linux endpoint management and Chromebook management.

Each purchased Windows/Mac/Linux license allows management of one FortiClient endpoint. You must purchase a minimum of 100 endpoint licenses, and you can have these EMS licenses for a maximum three year term. You can specify the number of endpoints and the term duration at time of purchase.

Each purchased Chromebook license allows management of one Google Chromebook user. You must purchase a minimum of 100 Google Chromebook user licenses and can have these EMS licenses for a maximum three year term. You can specify the number of Google Chromebook users and the term duration at time of purchase. FortiClient EMS uses one license seat per logged-in user. If the user logs out, the license seat times out (default timeout being 24 hours), and the license is released. At this point, another user can use this license seat.

You can use a licensed FortiClient EMS to deploy, provision, and manage FortiClient endpoints. However, if you have a FortiGate in your network, you can buy an add-on FortiGate endpoint license to enforce endpoint compliance on the firewall while EMS is managing the endpoints. Using FortiGate with EMS is optional.

An email is sent when you are running out of licenses. Additionally, a log entry is entered when a client is refused connection due to unavailable licenses.

Component applications

Common services or applications do not require a license.

During the installation of common services required for FortiClient EMS, you are not asked for license information.

Required services and ports

You must ensure required ports and services are enabled for use by FortiClient EMS and its associated applications on your server. The required ports and services enable FortiClient EMS to communicate with endpoints and servers running associated applications. You do not need to enable ports 8013 and 10443 as the FortiClient EMS installation opens these.

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
FortiClient Telemetry	FortiClient endpoint management	TCP	8013 (default)	Incoming	Installer/GUI
FortiClient upload	Used for FortiClient to upload events, logs, and diagnostics to FortiClient EMS.	TCP	8014 (default)	Incoming	GUI
Samba (SMB) service	FortiClient EMS uses the SMB service during FortiClient initial deployment.	TCP	445	Outgoing	N/A
Distributed Computing Environment / Remote Procedure Calls (DCE-RPC)	The EMS server connects to endpoints using RPC for FortiClient initial deployment.	TCP	135	Outgoing	N/A
Active Directory server connection	Retrieving workstation and user information	TCP	389 (LDAP) or 636 (LDAPS)	Outgoing	GUI
FortiClient download	Downloading FortiClient installer created by the EMS server	TCP	10443 (default)	Incoming	Installer
Apache/HTTPS	Web access to EMS	TCP	443	Incoming	Installer
FortiGuard	FortiGuard antivirus, vulnerability, and application version updates	TCP	80	Outgoing	N/A
SMTP server/email	Alerts for EMS and endpoint events. When an alert is triggered, an email notification is sent	TCP	25 (default)	Outgoing	GUI
FortiClient endpoint probing	FortiClient EMS uses ICMP for endpoint probing during FortiClient initial deployment.	ICMP	N/A	Outgoing	N/A

The following ports and services are only applicable when using FortiClient EMS to manage Chromebooks:

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
FortiClient on Chrome OS	Connection to EMS	TCP	8443 (default) You can customize this port.	Incoming	GUI
G suite API/Google domain directory	API calls to retrieve Google domain information	TCP	443	Outgoing	N/A

The following ports and services should be enabled for use on Chromebooks when using FortiClient for Chromebooks:

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
FortiClient EMS	Connection to profile server	TCP	8443 (default)	Outgoing	Via Google Admin console when adding the profile
FortiGuard	URL rating	TCP	443, 3400	Outgoing	N/A
FortiAnalyzer	Send logs to FortiAnalyzer	TCP	8443	Outgoing	N/A

For the list of required services and ports for FortiClient, see the *FortiClient Administration Guide* on the Fortinet Document Library.

Management capacity

FortiClient EMS is intended for use by enterprises. It has the capacity to manage a large number of endpoints. The following are suggested host system hardware configurations for FortiClient EMS. The suggested configurations depend on the number of endpoints FortiClient EMS is managing.

It is recommended to have at least 200 GB of disk space available.

Number of managed endpoints	Number of virtual CPUs	Memory (RAM) (in GB)	Suggested keep alive interval
Up to 10000	2	8	Default
10000 to 20000	4	8	Default
20000 to 30000	4	8	120 seconds
30000 to 40000	4	8	120 seconds
40000 to 50000	4	8	120 seconds
50000 to 75000	8	16	120 seconds

The requirements listed for managing 50000 to 75000 endpoints are considered best practice, even when managing a smaller number of endpoints.

For the purpose of this table, an Intel i5 processor with two cores and two threads per core is considered to have four virtual CPUs. An Intel i3 processor with two cores and one thread per core has two virtual CPUs.

FortiClient Telemetry security features

FortiClient connects to the FortiGate and EMS over an SSL connection. All protocol exchanges flow through this secure connection. The connection is closed after protocol exchanges between both parties are complete. The SSL connections require a valid certificate.

Telemetry connections between FortiClient and FortiGate or EMS may be configured to require a pre-shared password or connection key. See Configuring Endpoints settings on page 172 and Creating gateway lists on page 150.

The default Telemetry port number is 8013. This may be changed in EMS and FortiClient. When a port is not provided, FortiClient always attempt to connect to the default port, which is 8013. Changing this in EMS will lock out endpoints that are still using the default.

The EMS administrator may at anytime disconnect a rogue endpoint from EMS and prevent it from reconnecting to EMS in the future.

A list of TCP/IP ports used by the EMS is provided in Required services and ports on page 28. The network administrator may block all other ports or service requests to the EMS IP address or FQDN.

Server readiness checklist for installation

Use the following checklist to prepare your server for installation.

Checklist	Readiness factor
	Temporarily disable security applications. You must temporarily disable any antivirus software on the target server before you install FortiClient EMS. Installation may be slow or disrupted while these programs are active. Note a server may be vulnerable to attack when you uninstall or disable security applications.
	Consider the date and time settings you apply to your server. If managing Chromebooks, it is recommended to sync the time to the Google server time.
	Confirm required services and ports are enabled and available for use by FortiClient EMS.
	Ensure no conflict exists with port 443 for the Apache service to function properly.
	Ensure no conflict exists with ports 8013 and 8443 for the EMS service to function properly.

Upgrading from an earlier FortiClient EMS version

FortiClient EMS 6.0.1 supports upgrading from FortiClient EMS 1.0.3 and later 1.x versions. To ensure a successful upgrade, it is recommended you perform the upgrade on a staging server before upgrading the production server. Follow the procedure below.

1. (Optional) Back up the database from the EMS 1.x production server.
2. Install EMS 1.x on a staging server.
3. (Optional) Import the EMS 1.x database from the production server.
4. Connect FortiClient endpoints to the staging server.
5. Upgrade the staging server to EMS 6.0.1.
6. Monitor the staging server for two days.
7. Upgrade the production server to EMS 6.0.1.

Install preparation for managing Chromebooks

The following sections are only applicable if you plan to use FortiClient EMS to manage Chromebooks.

G Suite account

You need to sign up for your G Suite account before you can use the Google service and manage your Chromebook users.

The G Suite account is different from the free consumer account. The G Suite account is a paid account that gives access to a range of Google tools, services, and technology.

You can sign up for a G Suite account here: https://gsuite.google.com/signup/basic/welcome#0

In the sign up process, you must use your email address to verify your Google domain. This also proves you have ownership of the domain.

SSL certificates

FortiClient EMS requires an SSL certificate signed by a Certificate Authority (CA) in pfx format. Use your CA to generate a certificate file in pfx format, and remember the configured password. For example, the certificate file name is *server.pfx* with password 111111.

The server where FortiClient EMS is installed should have a fully qualified domain name (FQDN), such as ems.forticlient.com, and you must specify the FQDN in your SSL certificate.

If you are using a public SSL certificate, the FQDN can be included in *Common Name* or *Subject Alternative Name*. You must add the SSL certificate to FortiClient EMS. See Adding SSL certificates to FortiClient EMS on page 170. You do not need to add the root certificate to the Google Admin console.

If you are using a self-signed certificate (non-public SSL certificate), your certificate's *Subject Alternative Name* must include `DNS:<FQDN>`, for example, `DNS:ems.forticlient.com`. You must add the SSL certificate to FortiClient EMS and the root certificate to the Google Admin console to allow the extension to trust FortiClient EMS. See Adding root certificates on page 50.

Installation and Licensing

Before you install and license FortiClient EMS on a server, ensure you have:

- Reviewed Licenses on page 26
- Met the requirements listed in Required services and ports on page 28
- Completed the Server readiness checklist for installation on page 30
- Logged into the server as the administrator. The administrator user account is equivalent to a Windows administrator account and provides access to all common services, FortiClient EMS, and other application tasks. You can use this account to initially log into the server and to create other user accounts for normal day-to-day use of the applications.

It is recommended you install FortiClient EMS on a dedicated server in a controlled environment. Installing other software applications can interfere with normal operation of FortiClient EMS.

Downloading the installation file

FortiClient EMS is available for download from the following location:

Fortinet Support website: https://support.fortinet.com/

You can also receive the installation file from a sales representative.

The following installation file is available for FortiClient EMS:

```
FortiClientEnterpriseManagement_6.0.1.<build>_x64.exe
```

For information about obtaining FortiClient EMS, contact your Fortinet reseller.

Installing FortiClient EMS

The FortiClient EMS installation package includes:

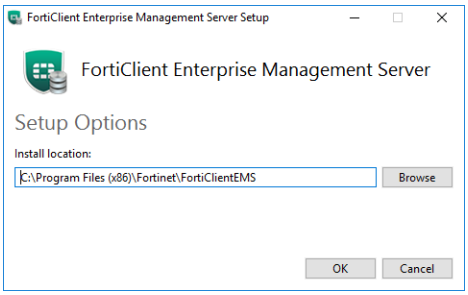
- FortiClient EMS
- Microsoft SQL Server 2014 Express Edition
- Apache HTTP server

Local administrator rights and Internet access are required to install FortiClient EMS.

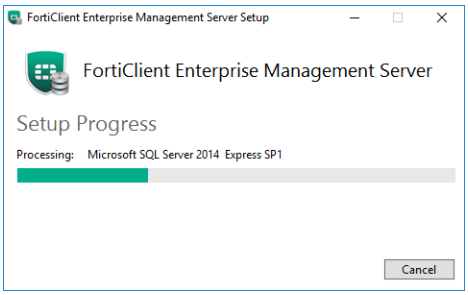
To install FortiClient EMS:

1. If you are logged into the system as an administrator, double-click the downloaded installation file.
   If you are not logged in as an administrator, right-click the installation file, and select *Run as administrator*.
2. If applicable, select *Yes* in the *User Account Control* window to allow the program to make changes to your system.
3. In the installation window, select *I agree to the license terms and conditions* if you agree with the license terms and conditions. If you do not agree, you cannot install the software.

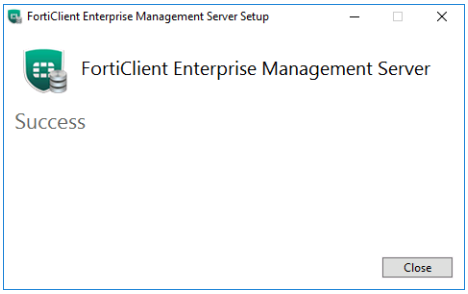
4. (Optional) Click *Options* to specify a custom directory for the FortiClient EMS installation.



   a. Click *Browse* to locate and select the custom directory.
   b. Click *OK* to return to the installation wizard.
5. Click *Install*.
   The installation may take 30 minutes or longer. It may appear to stop at times, but this is only because certain steps in the installation process take longer than others.



6. When the program has installed correctly, the *Success* window displays. Click *Close*.



A *FortiClient Enterprise Management Server* icon is added to the desktop.

Installing FortiClient EMS using the CLI

Installing FortiClient EMS using the CLI allows you to enable certain options during installation, such as customizing the SQL Server Express installation directory, using custom port numbers, and so on.

The following table provides a description of all options available when installing FortiClient EMS using the CLI. Note these options are case-sensitive:

Option	Description
`AllowedWebHostnames`	The default value is localhost, 127.0.0.1. To clear this value, first enter `AllowedWebHostnames=*`, then enter the desired AllowedWebHostnames value. Otherwise, the value entered will be appended to [localhost, 127.0.0.1], so that AllowedWebHostNames=localhost, 127.0.01, <new_value>.
`ApacheServerAdminEmail`	Enter the Apache Server administrator's email address. By default, this is admin@yourcompany.com.
`BackupDir`	Enter the desired backup directory path for SQL Server.
`ClientDownloadPort`	Enter the HTTP port number. The default is 80.
`RemoteManagementPort`	Enter the HTTPS port number. The default is 443.
`InstallFolder`	Specify the directory to install the default SQL Server Express instance.
`InstallSQL`	Controls whether the installer will install SQL Server Express on the same server as FortiClient EMS. Enter `1` to install SQL Server Express; otherwise, enter `0`. By default, SQL Server Express is installed with FortiClient EMS.
`ScriptDB`	Controls where the installer will attempt to create the database from db scripts. Enter `1` to create the database from db scripts. `0` should only be entered if databases have already been set up on the server and you are only installing EMS components locally.

Option	Description
ServerHostname	Enter the preferred host name (the remote host name). The default is the local host.
SQLAuthType	Enter sql.
SQLCmdlineOptions="/INSTANCEDIR"	Enter the desired directory to install SQL Server Express to.
SQLCmdlineOptions="/INSTANCENAME"	Enter the SQL Server instance name.
SQLEncryptConnection	(Optional) Enter yes to encrypt the connection to SQL Server. Otherwise, enter no. The default is yes.
SQLPort	Enter the port number the remote SQL Server instance is listening on. You should configure SQL Server to use a static port number.
SQLServer	Enter the DSN name of the computer where SQL Server is already installed.
SQLServerInstance	Enter the SQL Server instance name.
SQLService	If using a default database instance, enter the instance name. If using a named database instance, enter mssql$<instance_name>. For example, if your instance is named "database000", enter mssql$database000.
SQLTrustServerCertificate	(Optional) Enter yes to trust the SQL Server certificate on the machine where FortiClient EMS is installed. If entering no, you must install the issuing CA certificate of SQL Server's certificate onto the machine you are connecting FortiClient EMS from.
SQLUser	Enter the SQL username used to connect to the database instance. This must be pre-configured in SQL Server as described in .
SQLUserPassword	Enter the SQL password used to connect to the database instance.
WindowsUser	Enter the Windows username used to connect to the database instance. This must be pre-configured in SQL Server as described in .
WindowsUserPassword	Enter the Windows password used to connect to the database instance.

The following topics describe how to use the options above for specific use cases.

Allowing remote access to FortiClient EMS and using custom port numbers

To allow remote access to FortiClient EMS from a web browser, install FortiClient EMS by entering the following command in the CLI. You can also specify custom HTTP and HTTPS port numbers:

```
FortiClientEnterpriseManagement_6.0.1.XXXX_x64.exe ServerHostname=<preferred_host_name>
     ClientDownloadPort=<HTTP_port_number> RemoteManagementPort=<HTTPS_port_number>
```

```
AllowedWebHostnames=<allowed_web_host_names> ApacheServerAdminEmail=<Apache_Server_admin_
email_address>
```

The example below specifies the server host name as emshost.ems.com, appends emshost.ems.com to the allowed web host names, and specifies example@example.com as the Apache server administrator email. In this example, the HTTP and HTTPS ports are changed to 1080 and 22443, respectively.

```
FortiClientEnterpriseManagement_6.0.1.XXXX_x64.exe ServerHostname=emshost.ems.com
     ClientDownloadPort=1080 RemoteManagementPort=22443 AllowedWebHostnames=emshost.ems.com
     ApacheServerAdminEmail=example@example.com
```

Customizing the SQL Server Express install directory

By default, FortiClient EMS is installed with SQL Server Express. Using the CLI to install FortiClient EMS allows you to customize the SQL Server Express install directory.

Note these instructions are not applicable for SQL Server Enterprise or Standard, which must be installed separately from FortiClient EMS. For information on SQL Server Enterprise or Standard and FortiClient EMS, see Installing FortiClient EMS to specify SQL Server Enterprise or Standard instance on page 37.

Customizing the SQL Server Express install to a local directory

Use the following command to customize the SQL Server Express install to a local directory:

```
FortiClientEnterpriseManagement_6.0.1.XXXX_x64 SQLCmdlineOptions="/INSTANCENAME=FCEMS
     /INSTANCEDIR=<desired_directory>"
```

The example below installs FortiClient EMS, installing SQL Server to the C:\sqlserver directory:

```
FortiClientEnterpriseManagement_6.0.1.XXXX_x64 SQLCmdlineOptions="/INSTANCENAME=FCEMS
     /INSTANCEDIR=c:\sqlserver"
```

Customizing the SQL Server Express install to a remote directory

Use the following command to customize the SQL Server Express install to a remote directory:

```
FortiClientEnterpriseManagement_6.0.1.XXXX_x64 InstallFolder=<desired_directory>
     SQLServer=<SQL_Server_name> SQLServerInstance= SQLService=MSSQLSERVER
```

The example below installs FortiClient EMS, installing SQL Server to the C:\sqlserver directory on a computer with DNS name WIN-088:

```
FortiClientEnterpriseManagement_6.0.1.XXXX_x64 InstallFolder=c:/sqlserver SQLServer=WIN-0888
     SQLServerInstance= SQLService=MSSQLSERVER
```

Installing FortiClient EMS to specify SQL Server Enterprise or Standard instance

If you are using SQL Server Enterprise or Standard with FortiClient EMS, you must install FortiClient EMS using the CLI to specify the correct SQL Server instance. Ensure you have already installed and configured SQL Server Enterprise or Standard as detailed in .

Local existing database

This section lists the CLI commands for when FortiClient EMS and SQL Server Enterprise or Standard are installed on the same machine.

Database type	Command
Local default instance using SQL authentication	`FortiClientEnterpriseManagement_6.0.1.XXXX_x64.exe SQLUser=<username> SQLUserPassword=<password> InstallSQL=0 ScriptDB=1 SQLServerInstance= SQLService=<instance_name> SQLCmdlineOptions="/INSTANCENAME="`
Local default instance using local Windows authentication	`FortiClientEnterpriseManagement_6.0.1.XXXX_x64.exe SQLServerInstance= SQLService=<instance_name> SQLCmdlineOptions="/INSTANCENAME=" InstallSQL=0 ScriptDB=1`
Local named instance using SQL authentication	`FortiClientEnterpriseManagement_6.0.1.XXXX_x64.exe SQLUser=<username> SQLUserPassword=<password> InstallSQL=0 ScriptDB=1 SQLServerInstance=<instance_name> SQLService=mssql$<instance_name> SQLCmdlineOptions="/INSTANCENAME=<instance_name>"`
Local named instance using local Windows authentication	`FortiClientEnterpriseManagement_6.0.1.XXXX_x64.exe SQLServerInstance=<instance_name> SQLService=mssql$<instance_name> SQLCmdlineOptions="/INSTANCENAME=<instance_name>" InstallSQL=0 ScriptDB=1`

For example, if installing FortiClient EMS and pointing to a local instance named "database000" using SQL authentication, with SQL username "janedoe", password "password123", the command would be as follows:

```
FortiClientEnterpriseManagement_6.0.1.XXXX_x64.exe SQLUser=janedoe SQLUserPassword=password123
     InstallSQL=0 ScriptDB=1 SQLServerInstance=database000 SQLService=mssql$database000
     SQLCmdlineOptions="/INSTANCENAME=database000"
```

Remote existing database

Creating a backup directory

Prior to installing FortiClient EMS, create a backup directory on the database server and set the permissions as described below.

1. On the database server, create a backup directory.
2. Right-click the directory and select *Properties*.
3. On the *Security* tab, ensure all users have full control of the directory.

Installation commands for remote existing databases

For remote instances using Windows authentication (domain user), do the following:

1. Join the EMS and database servers to the same domain.
2. Create a database user that maps to the domain user.
3. In Local Group Policy Editor, add the domain user to the Log on as a service policy.

Database type	Command
Remote default or named instance using SQL authentication	`FortiClientEnterpriseManagement_6.0.1.XXXX_x64.exe SQLServer=<SQL_Server_name> SQLUser=<username> SQLUserPassword=<password> InstallSQL=0 ScriptDB=1 BackupDir=<backupdirectorypath>`
Remote default or named instance using Windows authentication (domain user)	`FortiClientEnterpriseManagement_6.0.1.XXXX_x64.exe SQLServer=<SQL_Server_name> WindowsUser=<username@domain.loc> WindowsUserPassword=<password> InstallSQL=0 ScriptDB=1 BackupDir=<backupdirectorypath>`

For example, if installing FortiClient EMS and pointing to a remote named instance on a computer with DNS name WIN-088 using Windows authentication, with Windows username "janedoe", password "password123", the command would be as follows. This example also includes the optional `SQLEncryptConnection` option:

```
FortiClientEnterpriseManagement_6.0.1.XXXX_x64.exe SQLServer=WIN-0888
     WindowsUser=janedoe@ems.loc WindowsUserPassword=password123 InstallSQL=0 ScriptDB=1
     BackupDir=c:\backup\ SQLEncryptConnection=no
```

Starting FortiClient EMS and logging in

FortiClient EMS runs as a service on Windows computers.

To start FortiClient EMS:

1. Double-click the *FortiClient Enterprise Management Server* icon.
2. Sign in with the username *admin* and no password.
3. Change the username and password by going to *Administration* > *Administrators*.
4. Configure FortiClient EMS by going to *System Settings*.

Accessing FortiClient EMS remotely

You can access FortiClient EMS remotely using a web browser instead of the GUI.

To enable remote access to FortiClient EMS:

1. Go to *System Settings* > *Server*.
2. Enable *Remote HTTPS access*.
3. If desired, in the *Custom hostname* box, type the host name or IP address. Otherwise, the *Pre-defined hostname* is used.
4. If desired, select the *Redirect HTTP request to HTTPS* checkbox. If this option is enabled, if you attempt to remotely access EMS at *http://<server_name>*, this is automatically redirected to *https://<server_name>*.
5. Click *Save*.

To remotely access FortiClient EMS:

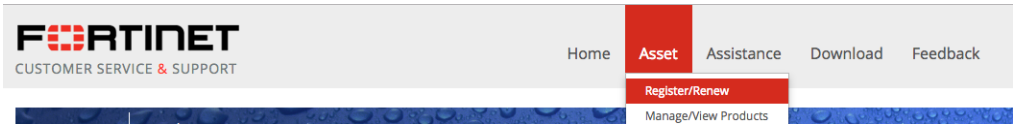
- To access EMS from the EMS server, visit `https://localhost`
- To access the server remotely, use the server's hostname: `https://<server_name>`
  Ensure you can ping `<server_name>` remotely. This can be achieved by adding it into a DNS entry or to the Windows hosts file. You may have to modify the Windows firewall rules to allow the connection.

Licensing FortiClient EMS

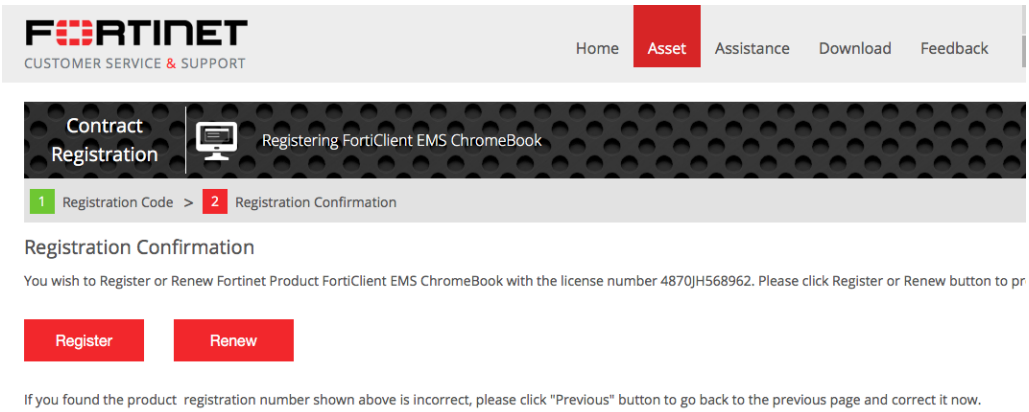
An instructional video on how to obtain licensing for FortiClient EMS is available in the Fortinet Video Library.

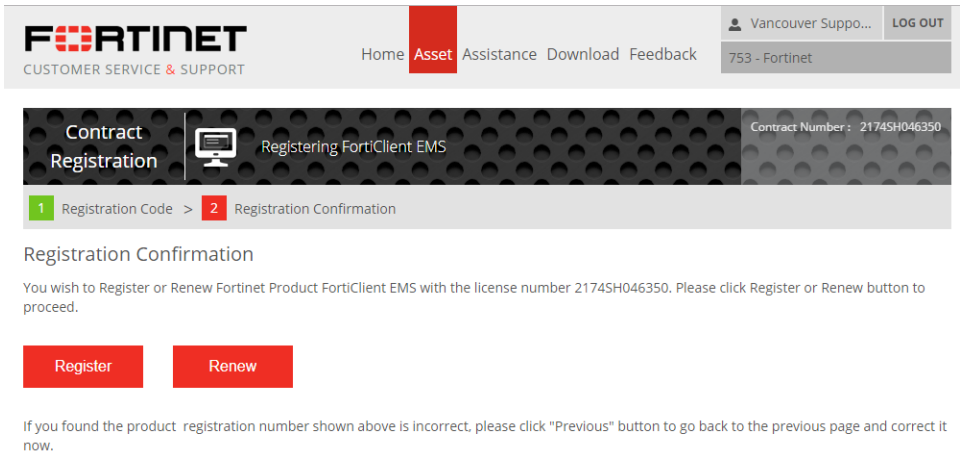
To license FortiClient EMS:

1. Purchase FortiClient EMS from a reseller.
   You can visit fortinet.com/partners.html to find a reseller. Once you purchase FortiClient EMS, you receive the *Service Registration Document* via email. This email contains the *Contract Registration Code* used to obtain the FortiClient EMS license.
2. Log into the Fortinet Support website.
3. Register FortiClient EMS:
   a. Go to *Asset* > *Register/Renew*.



   b. In the *Specify Registration Code* field, enter the *Contract Registration Code*. This is the number received in the license email from Fortinet.
   c. Select the end user type, then click *Next*.
   d. Click *Register*.

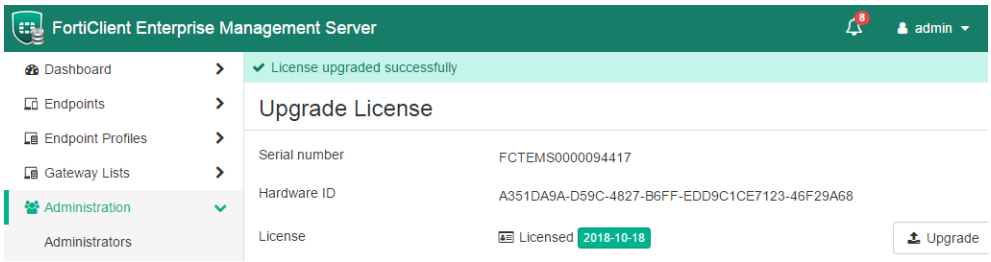




If you have not registered an EMS device, you are prompted to do so. This requires obtaining the *Hardware ID* from FortiClient EMS. You can obtain the *Hardware ID* by going to *Administration* > *Upgrade License* > *Hardware ID*.

e. In the *Product Description* field, enter a product description if desired, then enter the *Hardware ID*.
f. Select the *Fortinet Partner* reseller, then click *Next*.
g. Read, verify, and agree to the service's *Terms and Conditions*, then click *Next*.
h. Verify the *Product Entitlement* list for your FortiClient EMS purchase. Select the *BY ACCEPTING THESE TERMS...* checkbox, then click *Confirm*. The license file is now available to use with your FortiClient EMS installation.
i. Click *Finish*.

4. Retrieve the license key:
   a. Go to *Asset* > *Manage/View Products*. Select FortiClient EMS.
   b. From the left panel, select *License & Key*.
   c. From the *Available Key(s)* list, click *Get The License File* for FortiClient EMS.
5. License FortiClient EMS:
   a. From FortiClient EMS, go to *Administration* > *Upgrade License*. Click the *Activate* button.
   b. Click the *Browse* button, select the license file, and click *Upload*. You have successfully licensed FortiClient EMS.



To upgrade or renew your license, contact Fortinet Support.

License status

The *Dashboard* > *FortiClient Status* > *System Information* widget displays your license status. Your license status can change. The options are:

License Status	Description
Trial	If you just installed FortiClient EMS, the trial license is enabled by default. You should upload the license file you purchased.
Non-expired license	You can upgrade the license. See License upgrades or renewals on page 165.
Expired license	You can renew the license. See License upgrades or renewals on page 165. Note you have 10 days after the license expiry date to renew the license. After 10 days, FortiClient EMS reverts to trial mode.

Extending license expiries

You can apply multiple licenses to FortiClient EMS to extend the license expiry. For example, consider you purchase two one-year licenses for FortiClient EMS. After you register and apply the first license, FortiClient EMS has an expiry date of September 5, 2018. You can register and apply the second license as a renewal, after which FortiClient EMS has an expiry date of September 5, 2019.

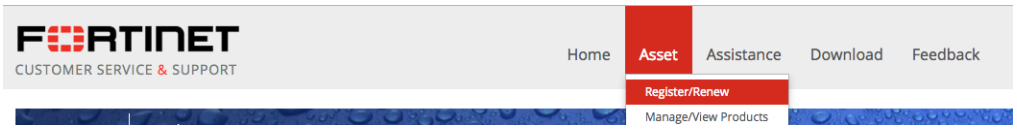
Note you must upload the second license file to FortiClient EMS using the GUI. Registering the license does not automatically update the license expiry in FortiClient EMS.

Using a second license to extend the license expiry date does not increase the number of licensed clients. To increase the number of licensed clients, contact Fortinet Support for a co-term contract.

To extend a license expiry:

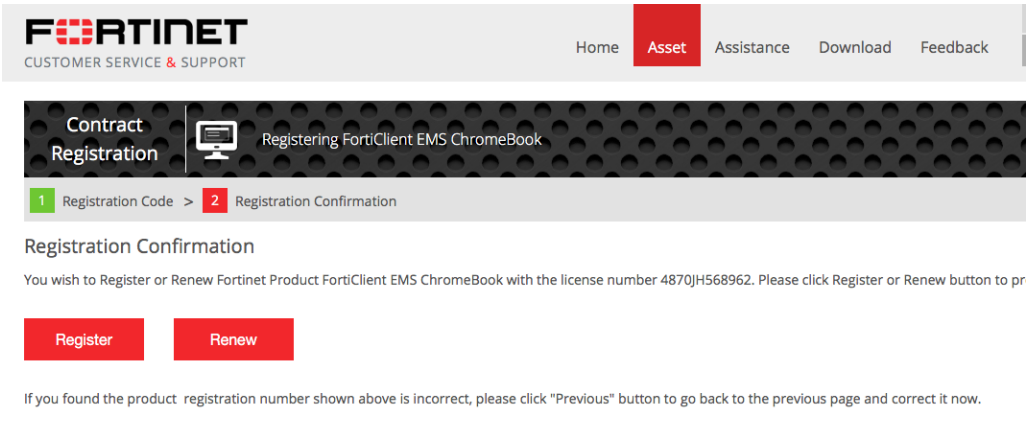
1. Purchase two FortiClient EMS licenses separately from a reseller. You must purchase the licenses separately to ensure there are two registration codes. Otherwise, you cannot stack the licenses.

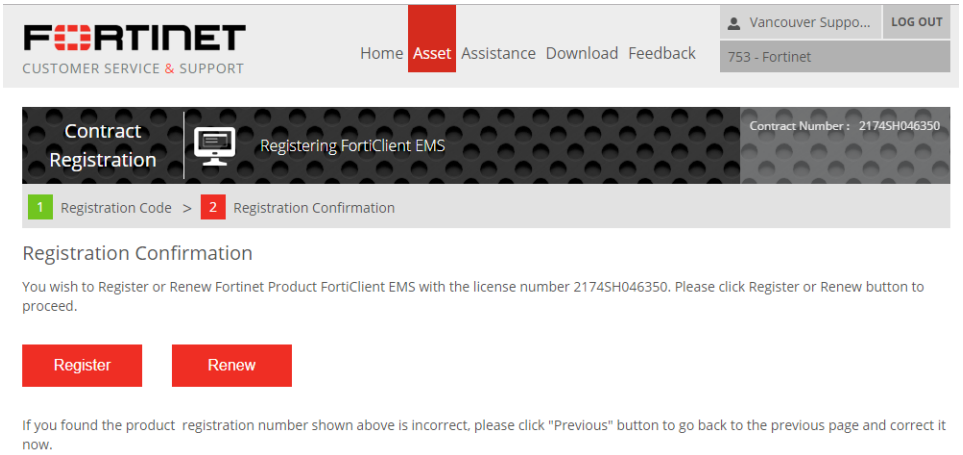
   You can visit fortinet.com/partners.html to find a reseller. Once you purchase FortiClient EMS, you receive the *Service Registration Document* via email. This email contains the *Contract Registration Code* used to obtain the FortiClient EMS license.
2. Register and apply the first license to FortiClient EMS as described in Licensing FortiClient EMS on page 40.
3. Register the second license:
   a. Log into the Fortinet Support website.
   b. Go to *Asset* > *Register/Renew*.



   c. In the *Specify Registration Code* field, enter the *Contract Registration Code*. This is the number received in the license email from Fortinet.
   d. Select the end user type, then click *Next*.

e. In the *Registration Confirmation* window, click *Renew*.



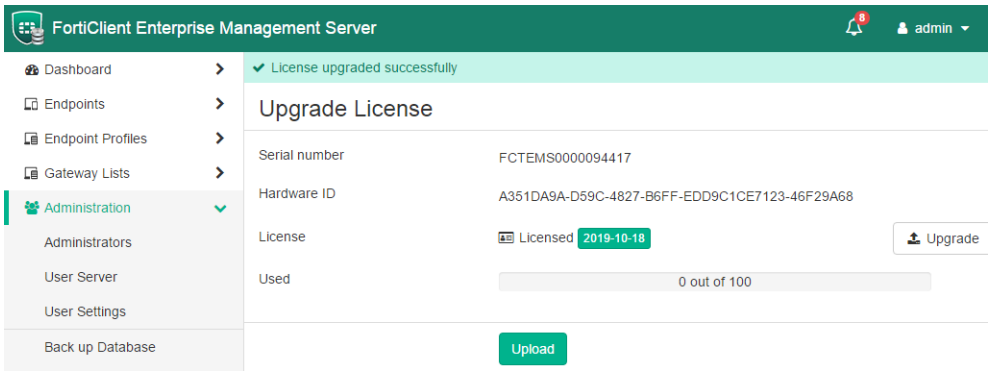


f. In the *Specify Fortinet Registration Information* window, do one of the following. You can find the serial number in the *System Information* widget in FortiClient EMS.
   i. Enter the serial number in the *The Product Serial Number is* field.
   ii. Select the desired serial number in the *Product SN* list.

g. Read, verify, and agree to the service's *Terms and Conditions*.

4. Retrieve the license key:
   a. Go to *Asset* > *Manage/View Products*. Select FortiClient EMS.
   b. From the left panel, select *License and Key*.
   c. From the *Available Key(s) List*, select the FortiClient EMS entry. Then, click *Get The License File*.
5. License FortiClient EMS:
   a. From FortiClient EMS, go to *Administration* > *Upgrade License*, then click *Activate*.
   b. Click *Browse*, select the license file, and click *Upload*. You have successfully extended the license for FortiClient EMS. The expiry date displayed in the *System Information* widget updates to a year after the

initial license expiry date.



Help with licensing

For licensing issues with FortiClient EMS, contact the licensing team at Fortinet Technical Assistance Center (TAC):

- Phone: +1-866-648-4638
- Technical support: support.fortinet.com/

Specifying different ports

In cases where there are pre-existing services running on default FortiClient EMS ports, you can specify another port using the CLI to run the installer. You can use the following commands:

Command	Description
`ClientDownloadPort`	Port used to download FortiClient from FortiClient EMS.
`RemoteManagementPort`	Port used for EMS administration.

Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise

FortiClient EMS is installed with Microsoft SQL Server Express, which has a file size limit of 10 GB per database. Log entries recorded in the database are rotated on a schedule of seven days (one week) by default. If the FortiClient deployment is large, the database size may reach the 10 GB limit over time. The FortiClient EMS administrator may upgrade the default SQL Server installation from Express to Standard or Enterprise edition. The database file size limit for these editions is in the PB range, which is unlimited for most practical usage.

Microsoft SQL Server Express is free. All other editions require a license from Microsoft.

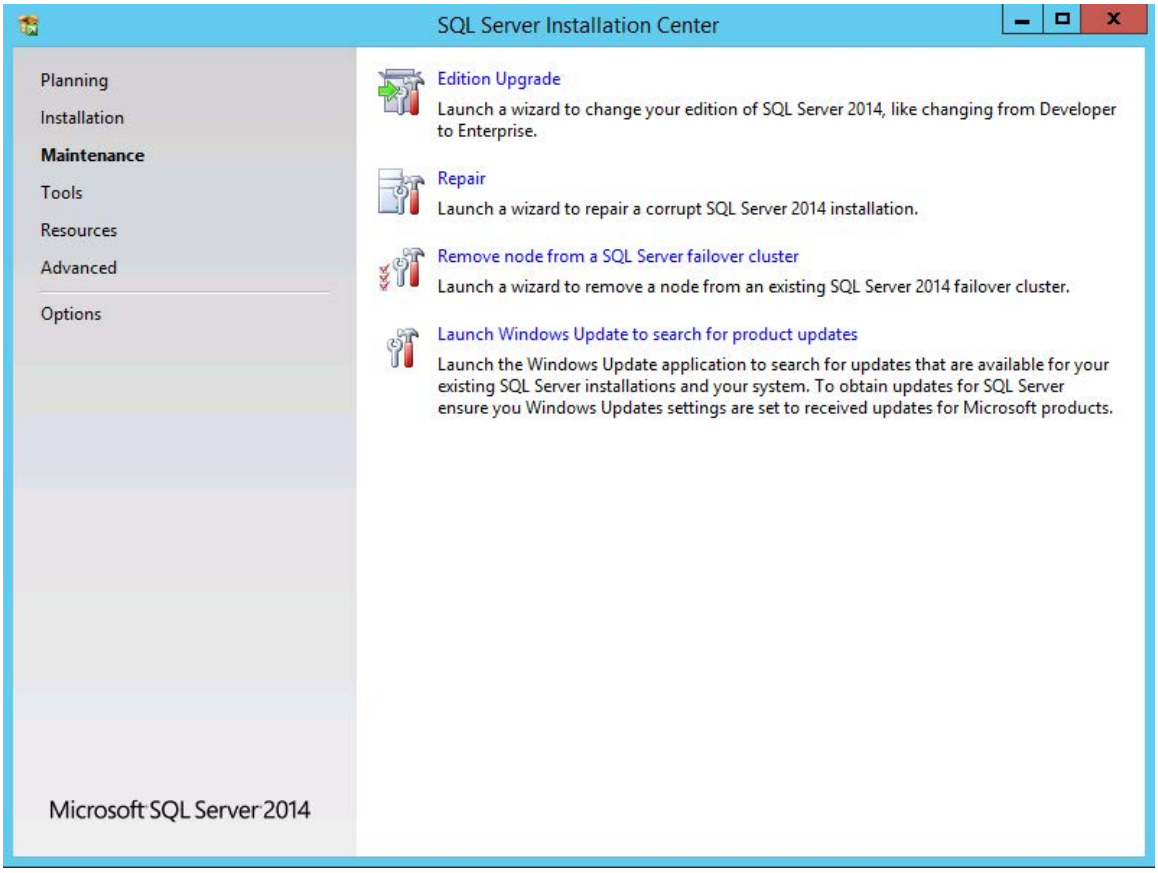
See the following Microsoft documentation on upgrading between editions called *Upgrade to a Different Edition of SQL Server 2014 (Setup)* at https://technet.microsoft.com/en-us/library/cc707783(v=sql.120).aspx

The EMS database is saved in the *C:\Program Files\Microsoft SQL Server\MSSQL12.FCEMS\MSSQL\DATA\FCM_root.mdf* file in the EMS host server. This file's size should remain below the 10 GB limit for Microsoft SQL Server Express.

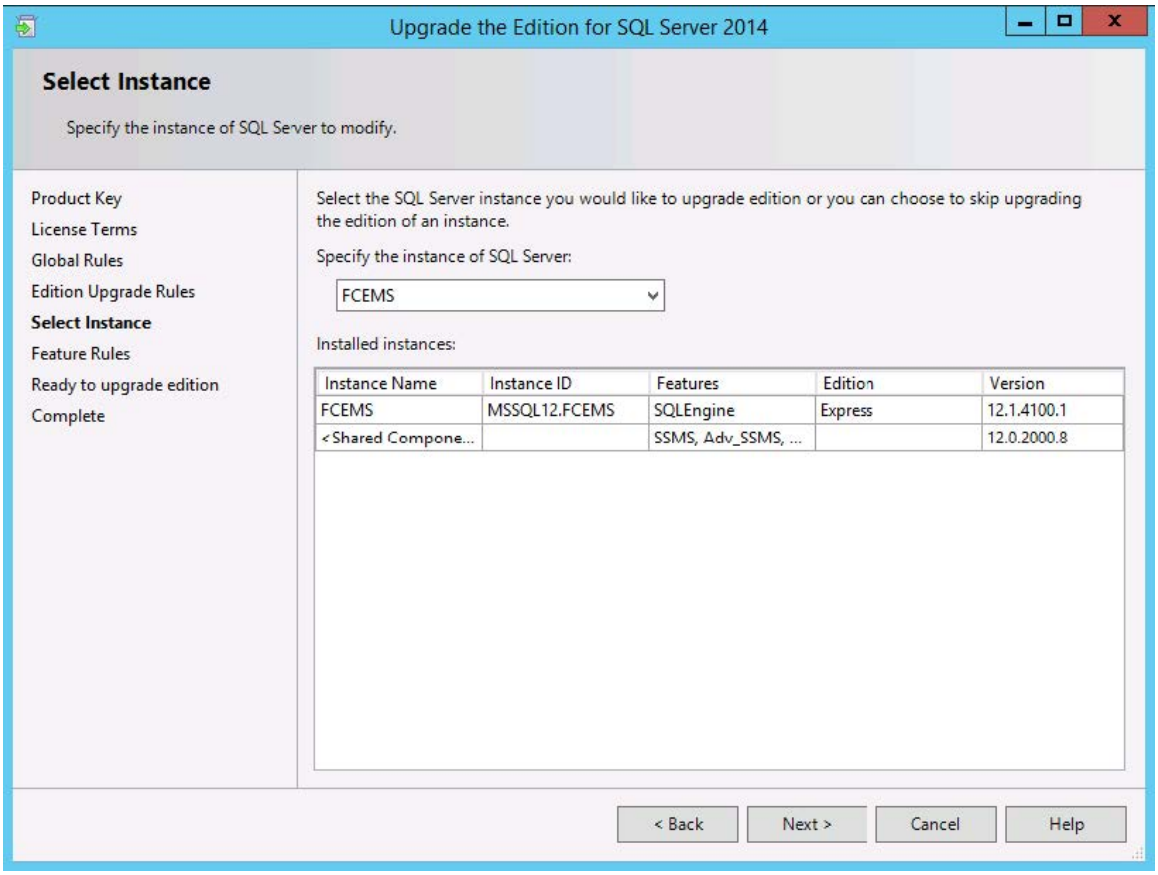
It is recommended to do a database edition upgrade outside normal production hours.

To upgrade Microsoft SQL Server Express:

1. Attach the SQL Server 2014 installation media to the FortiClient EMS server.
   The installation media is a DVD or ISO file. If using the DVD, insert the DVD into the EMS host computer (host server). If your host server is a virtual machine, use the ISO file.
2. Run the SQL Server setup application wizard.
3. In the *SQL Server Installation Center* wizard, go to *Maintenance* > *Edition Upgrade*.



4. Enter the *product key*.
5. Accept the license terms, then click *Next*.
6. Under *Select Instance*, in the *Specify the instance of SQL Server* dropdown list, select *FCEMS*. Then, click *Next*.



7. Under *Ready to upgrade edition*, click *Upgrade*.
8. After the upgrade is complete, click *Finish*.

Testing the SQL server upgrade

It is recommended to run a short test on FortiClient EMS after the upgrade to verify proper operations. A simple test may be to:

1. Connect FortiClient on one or two test endpoints to FortiClient EMS.
2. Create a new custom group in FortiClient EMS and add the test endpoints to it.
3. Create a new endpoint profile and assign it to the new custom group.
4. Check that FortiClient on the test endpoints received the new profile.

Monitor the system closely over the first few days for any unusual behavior.

Uninstalling FortiClient EMS

Use the *Programs and Features* pane of the Microsoft Windows Control Panel to uninstall FortiClient EMS.

FortiClient EMS installs the following dependencies. If other applications on the same computer are not using them, you can uninstall them manually after removing FortiClient EMS.

- Microsoft ODBC Driver 11 for SQL Server
- Microsoft SQL Server 2008 Setup Support Files
- Microsoft SQL Server 2012 Native Client
- Microsoft SQL Server 2014 (64-bit)
- Microsoft SQL Server 2014 Setup (English)
- Microsoft SQL Server 2014 Transact-SQL ScriptDom
- Microsoft Visual C++ 2010 x64 Redistributable – 10.0
- Microsoft Visual C++ 2010 x86 Redistributable – 10.0
- Microsoft Visual C++ 2013 x86 Redistributable – 12.0
- Microsoft VSS Writer for SQL Server 2014
- SQL Server Browser for SQL Server 2014

To uninstall FortiClient EMS:

1. Select *Start* > *Control Panel* > *Programs* > *Uninstall a program*.
2. Select *FortiClient Enterprise Management Server*, and click *Uninstall*.
3. Follow the uninstallation wizard prompts.

Chromebook-only Setup

The following sections are only applicable if you plan to use FortiClient EMS to manage Chromebooks.

Google Admin Console setup

This section describes how to add and configure the FortiClient Web Filter extension on Chromebooks enrolled in the Google domain.

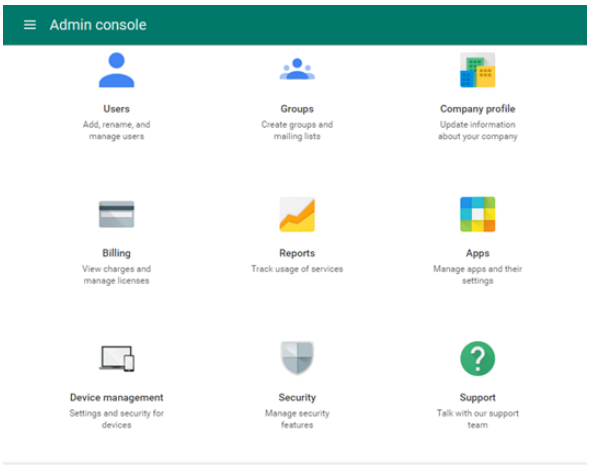
Following is a summary of how to set up the Google Admin console:

1. Log into the Google Admin console. See Logging into the Google Admin console on page 48.
2. Add the FortiClient Web Filter extension. See Adding the FortiClient Web Filter extension on page 49.
3. Configure the FortiClient Web Filter extension. See Configuring the FortiClient Web Filter extension on page 49.
4. Add the root certificate. See Adding root certificates on page 50.

Logging into the Google Admin console

To log into the Google Admin console:

1. Log into the Google Admin console (https://admin.google.com) using your Google domain admin account.
   The Admin console displays.

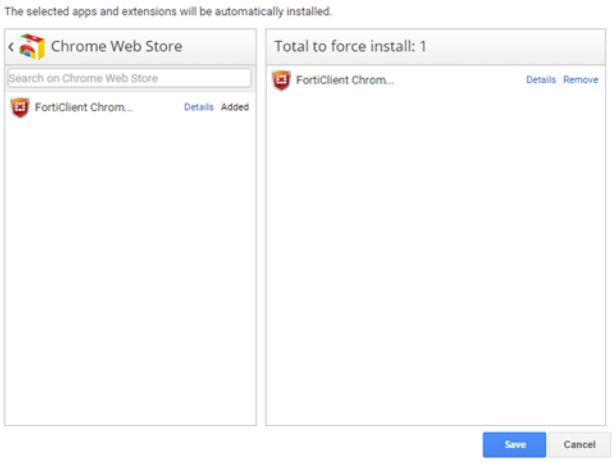


Adding the FortiClient Web Filter extension

FortiClient EMS software is not available for public use. You can only enable the feature using the following extension ID: igbgpehnbmhgdgjbhkkpedommgmfbeao

To add the FortiClient Web Filter extension:

1. In the Google Admin console, go to *Device management* > *Chrome Management* > *User Settings* > *Apps and Extensions* > *Force-installed Apps and Extensions* > *Manage force-installed apps*.
2. Select *Chrome Web Store*, and search for the following extension ID: igbgpehnbmhgdgjbhkkpedommgmfbeao.
3. Add the extension ID and save.
   The extension name displays as *FortiClient Chromebook Web Filter Extension*.



Configuring the FortiClient Web Filter extension

You must configure the FortiClient Chromebook Web Filter extension to enable the Google Admin console to communicate with FortiClient EMS.

FortiClient EMS hosts the services that assign endpoint profiles of web filtering policies to groups in the Google domain. FortiClient EMS also handles the logs and web access statistics sent from the FortiClient Web Filter extensions.

FortiClient EMS is the profile server.

To configure the FortiClient Web Filter extension:

1. In FortiClient EMS, locate the server name and port by going to *System Settings* > *Server*.
2. Create a text file that contains the following text:

```
{
   "ProfileServerUrl": { "Value": "https://< ProfileServer >:< port for Profile Server >"}
```

```
}
```

For example:

```
{
   "ProfileServerUrl": { "Value": "https://ems.mydomain.com:8443"}
}
```

3. In the Google Admin console, go to *Device management* > *Chrome Management* > *App Management* > *FortiClient Chrome Web Filter Extension* > *User settings*.
4. Click a domain or organization unit (OU).
5. In the right pane, under *Configure*, upload a new configuration file.

   You can also view the current settings.
6. Click *Save*.
7. Go to *Device Management* > *Chrome* > *App Management* to view your configured Chrome apps.

Adding root certificates

This section includes the following information.

- Communication with the FortiClient Chromebook Web Filter extension on page 50
- Communication with FortiAnalyzer for logging on page 50
- Summary of where to add certificates on page 52
- Uploading root certificates to the Google Admin console on page 52

Communication with the FortiClient Chromebook Web Filter extension

The FortiClient Chromebook Web Filter extension communicates with FortiClient EMS using HTTPS connections. The HTTPS connections require an SSL certificate. You must obtain an SSL certificate and add it to FortiClient EMS to allow the extension to trust FortiClient EMS.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiClient EMS. See Adding SSL certificates to FortiClient EMS on page 170.

However, if you prefer to use a certificate not from a common CA, you must add the SSL certificate to FortiClient EMS and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiClient EMS will not work. See Uploading root certificates to the Google Admin console on page 52.

Communication with FortiAnalyzer for logging

This section applies only if you are sending logs from FortiClient EMS to FortiAnalyzer. If you are not sending logs, skip this section.

Sending logs to FortiAnalyzer requires you enable ADOMs in FortiAnalyzer and add FortiClient EMS to FortiAnalyzer. FortiClient EMS is added as a device to the FortiClient ADOM in FortiAnalyzer. See the *FortiAnalyzer Administration Guide*.

FortiClient EMS supports logging to FortiAnalyzer. If you have a FortiAnalyzer device and configure FortiClient EMS to send logs to FortiAnalyzer, a FortiAnalyzer CLI command must be enabled and an SSL certificate is required to support communication between the FortiClient Web Filter extension and FortiAnalyzer.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiAnalyzer. See Adding SSL certificates to FortiAnalyzer.

However, if you prefer to use a certificate not from a common CA, you must add the SSL certificate to FortiAnalyzer and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiAnalyzer will not work. See Uploading root certificates to the Google Admin console on page 52.

The FortiAnalyzer IP address should be specified in the SSL certificate. If you are using a public SSL certificate, the FortiAnalyzer IP address can be assigned to *Common Name* or *Alternative Name*. If you are using a self-signed (nonpublic) SSL certificate, your certificate's *Subject Alternative Name* must include `IP:<FortiAnalyzer IP>`.

Enabling HTTPS logging access to FortiAnalyzer

You must use the FortiAnalyzer CLI to add HTTPS-logging to the allow-access list in FortiAnalyzer. This command is one step in the process that allows FortiAnalyzer to receive logs from FortiClient EMS.

In FortiAnalyzer CLI, enter the following command:

```
config system interface
   edit "port1"
      set allowaccess https ssh https-logging
   next
end
```

Adding SSL certificates to FortiAnalyzer

To add SSL certificates to FortiAnalyzer:

1. In FortiAnalyzer, go to *System Settings* > *Certificates* > *Local Certificates*.
2. Click *Import*. The *Import Local Certificate* dialog appears.
3. In the *Type* list, select *Certificate* or *PKCS #12 Certificate*.
4. Beside *Certificate File*, click *Browse* to select the certificate.
5. Enter the password and certificate name.
6. Click *OK*.

Selecting certificates for HTTPS connections

To select certificates for HTTPS connections:

1. In FortiAnalyzer, go to *System Settings* > *Admin* > *Admin Settings*.
2. In the *HTTPS & Web Service Certificate* box, select the certificate to use for HTTPS connections, and click *Apply*.

Summary of where to add certificates

The following table summarizes where to add certificates to support communication with the FortiClient Web Filter extension and FortiAnalyzer.

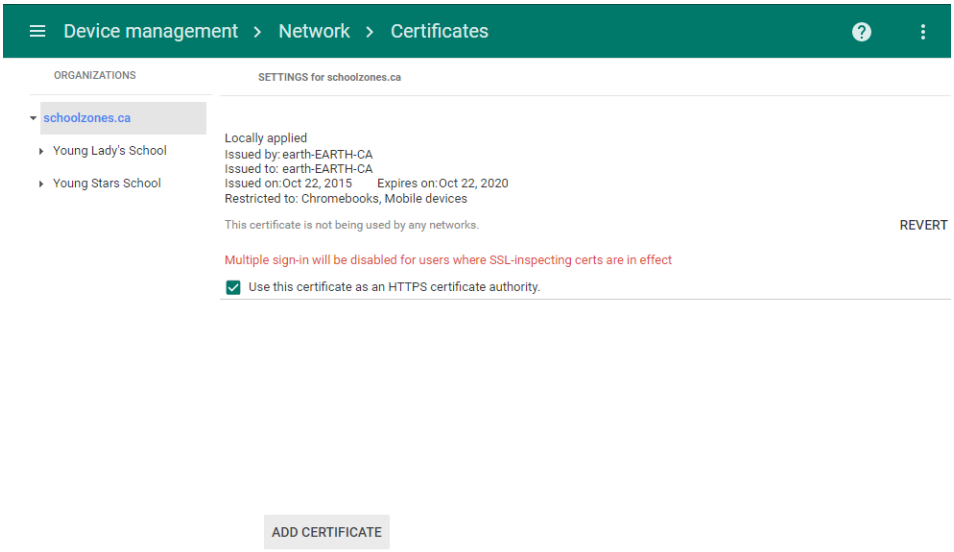
Scenario	Certificate and CA	Where to add certificates
Allow the FortiClient Chromebook Web Filter extension to trust EMS	Public SSL certificate	• Add SSL certificate to FortiClient EMS.
	SSL certificate not from a common CA	• Add SSL certificate to FortiClient EMS. • Add your certificate's root CA to the Google Admin console.
Allow the FortiClient Chromebook Web Filter extension to trust FortiAnalyzer for logging	Public SSL certificate	• Add SSL certificate to FortiAnalyzer.
	SSL certificate not from a common CA	• Add SSL certificate to FortiAnalyzer. • Add your certificate's root CA to the Google Admin console.

Uploading root certificates to the Google Admin console

To add root certificates:

1. In the Google Admin console, go to *Device Management* > *Network* > *Certificates (root certificate) (crt certificate)*.
2. Add the root certificate.
3. Select the *Use this certificate as an HTTPS certificate authority* checkbox.

Do not forget to select the *Use this certificate as an HTTPS certificate authority* checkbox.



Disabling access to Chrome developer tools

It is recommended to disable access to Chrome developer tools. This blocks users from disabling the FortiClient Web Filter extension.

To disable access to Chrome developer tools:

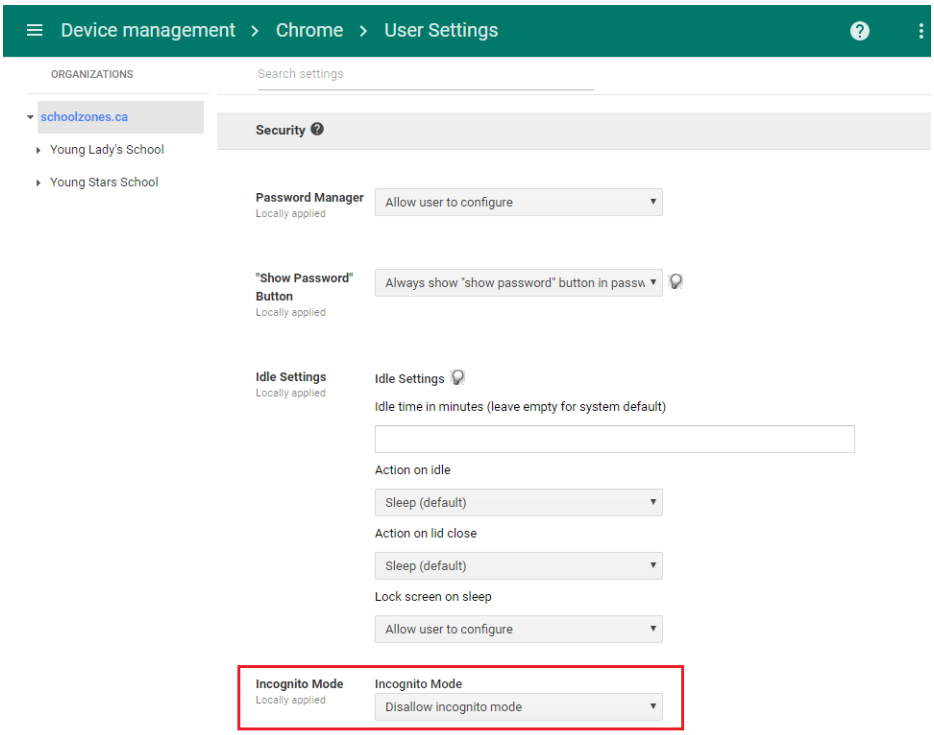
1. In the Google Admin console, go to *Device management* > *Chrome Management* > *User Settings*.
2. For the *Developer Tools* option, select *Never allow use of built-in developer tools*.

Disallowing incognito mode

When users browse in incognito mode, extensions are bypassed. Incognito mode should be disallowed for managed Google domains.

To disallow incognito mode:

1. In the Google Admin console, go to *Device management* > *Chrome management* > *User settings*.
2. From the left panel, select the organization.
3. In the *Security* section, set *Incognito Mode* to *Disallow incognito mode*.



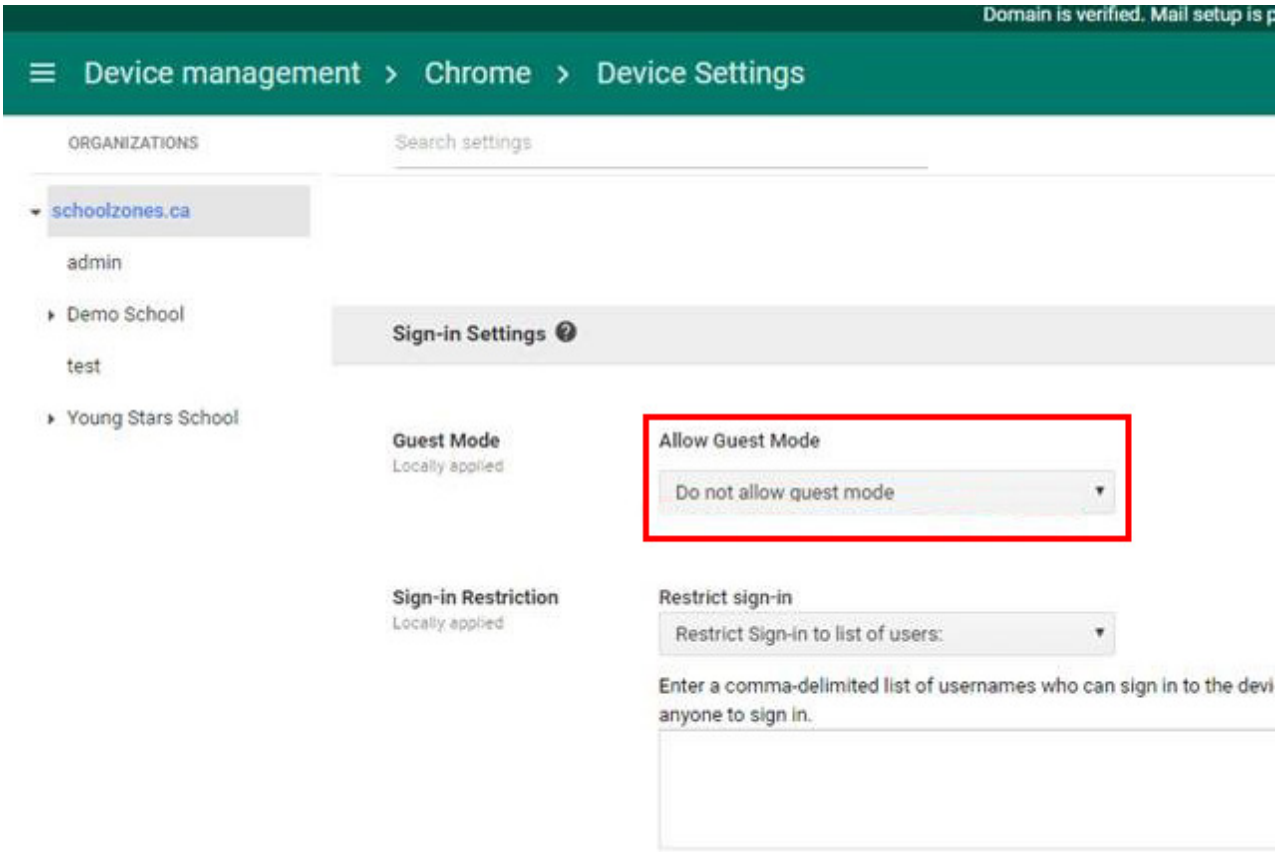
4. Click *Save*.

Disallowing guest mode

Guest mode should be disallowed for managed Google domains.

To disallow guest mode:

1. In the Google Admin console, go to *Device management* > *Chrome management* > *Device settings* > *Sign-in settings*.
2. From the left panel, select the organization.
3. Under *Guest Mode*, select *Do not allow guest mode* from the *Allow Guest Mode* dropdown list.



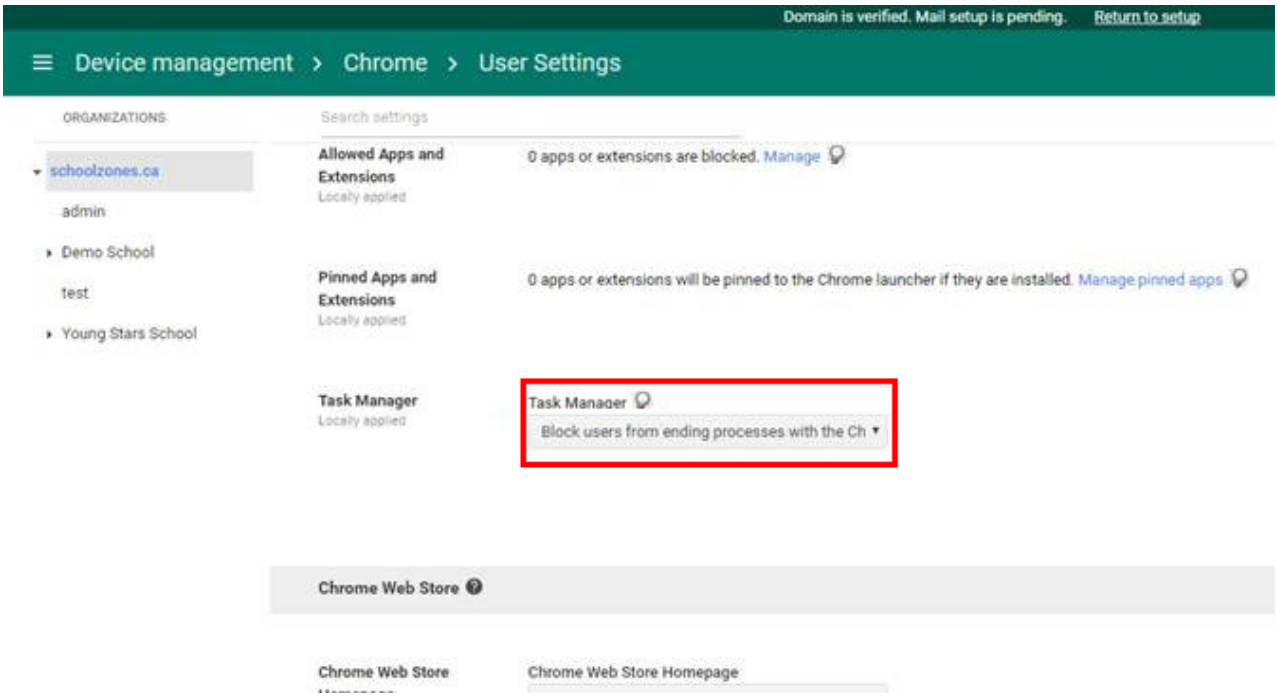
4. Click *Save*.

Blocking Task Manager

Task Manager should be blocked for managed Google domains.

To block Task Manager:

1. In the Google Admin console, go to *Device Management* > *Chrome Management* > *User settings* > *Apps and Extensions*.
2. From the left panel, select the organization.
3. Under *Task Manager* select *Block users from ending processes with the Chrome Task Manager* from the dropdown list.



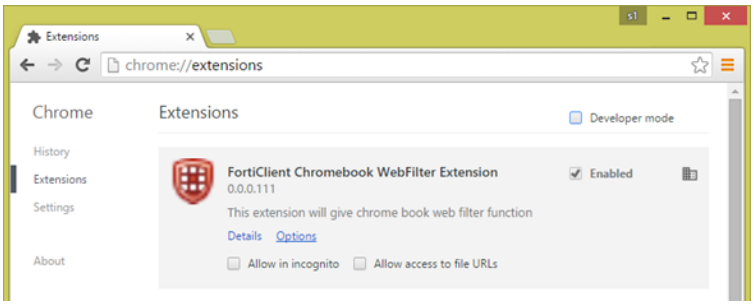
4. Click *Save*.

Verifying the FortiClient Web Filter extension

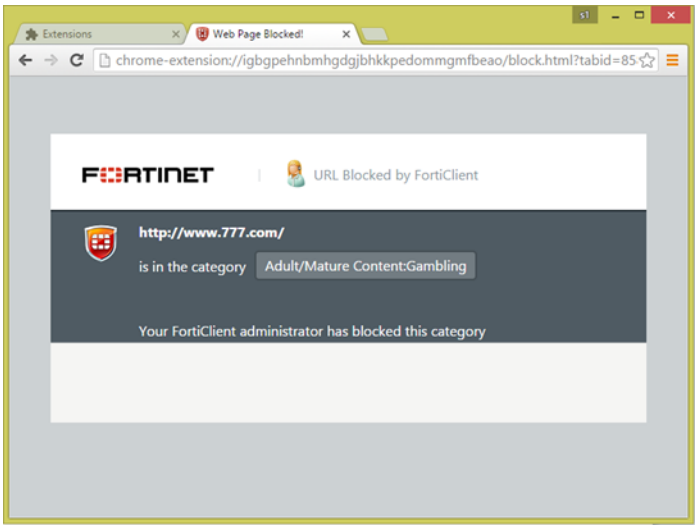
After you add the Google domain to FortiClient EMS, the Google Admin console automatically pushes the FortiClient Web Filter extension to the Chromebooks when users log into the Google domain. You can verify the feature has become available on the Chromebooks.

To verify that the extension is installed:

1. Open the Google Chrome browser.
2. Type the following in the address bar: *chrome://extensions*



3. Visit any gambling site, such as http://www.777.com, and confirm the site is blocked.



Service account credentials

FortiClient EMS requires service account credentials generated by the Google Developer console. You can use the default service account credentials provided with FortiClient EMS or generate and use unique service account credentials, which is more secure.

The service account credentials must be the same in FortiClient EMS and the Google Admin console.

This section describes how to configure default and unique service account credentials. See the following sections.

Configuring default service account credentials

FortiClient EMS includes the following default service account credentials generated by the Google Developer console:

Option	Default setting	Where used
Client ID	102515977741391213738	Google Admin console
Email address	account-1@forticlientwebfilter.iam.gserviceaccount.com	FortiClient EMS
Service account certificate	A certificate in `.pem` format for the service account credentials	FortiClient EMS

The service account credentials are a set. If you change one credential, you must change the other two credentials.

Adding the default service account client ID to the Google Admin console

To configure the default service account credentials, you must add the client ID's default value to the Google Admin console. No other configuration for service account credentials is required. See Adding service account credentials to the Google Admin console on page 61.

Configuring unique service account credentials

When using unique service account credentials for improved security, you must complete the following steps to add the unique service account credentials to the Google Admin console and FortiClient EMS:

1. Create unique service account credentials using the Google Developer console. See Creating unique service account credentials on page 57.
2. Add the unique service account credentials to the Google Admin console. See Adding service account credentials to the Google Admin console on page 61.
3. Add the unique service account credentials to FortiClient EMS. See Adding service account credentials to EMS on page 61.

Creating unique service account credentials

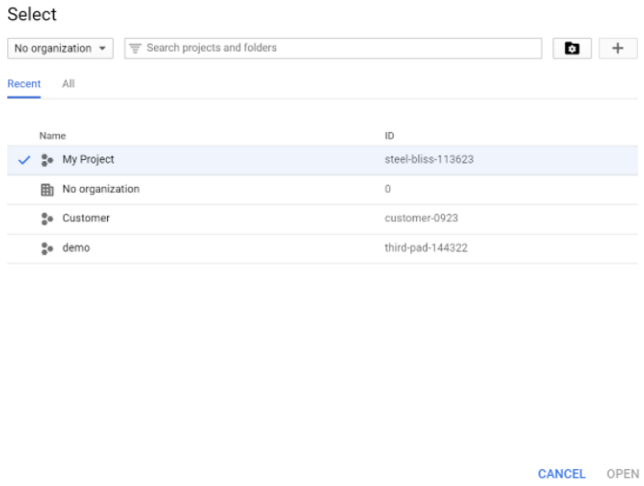
Creating a unique set of service account credentials provides more security. Unique service account credentials include the following:

- Client ID (a long number)
- Service account ID (email address)
- Service account certificate (a certificate in `.pem` format)

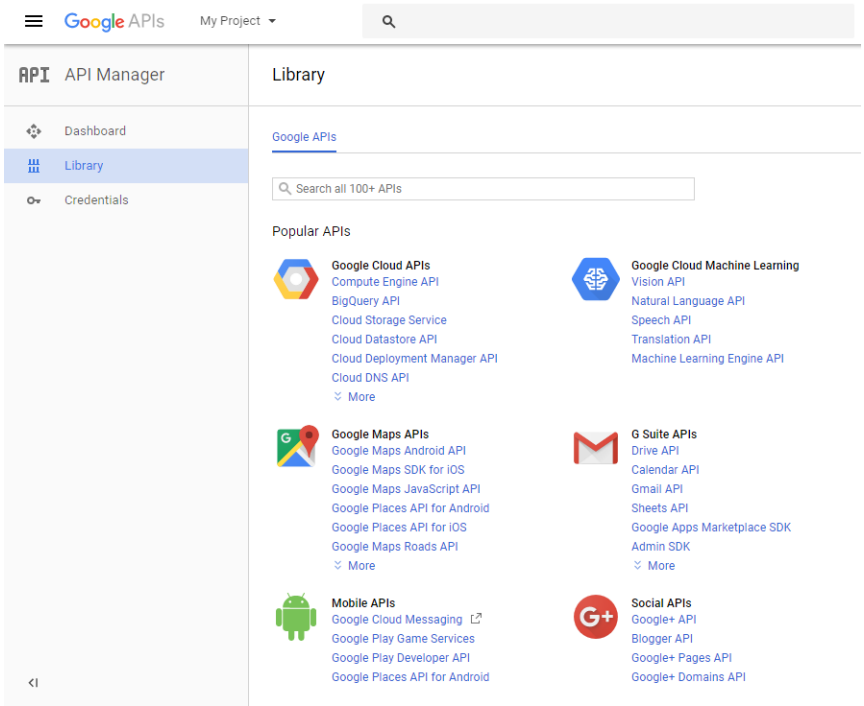
To create a unique service account:

1. Go to https://console.developers.google.com.
2. Log in with your G Suite account credentials.

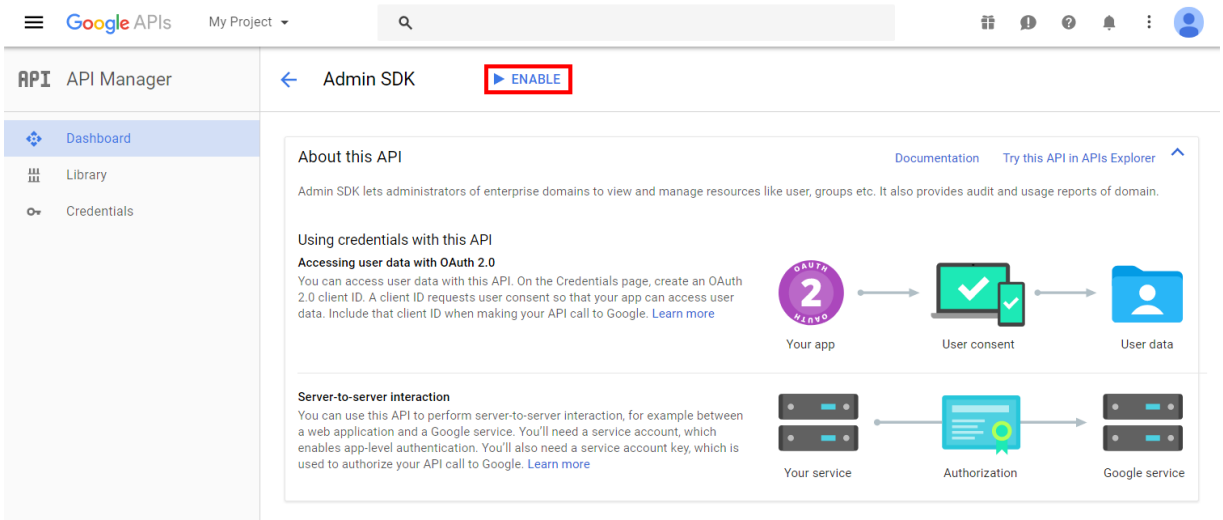
3. Create a new project:
   a. Click the toolbar list. The browser displays the following dialog.



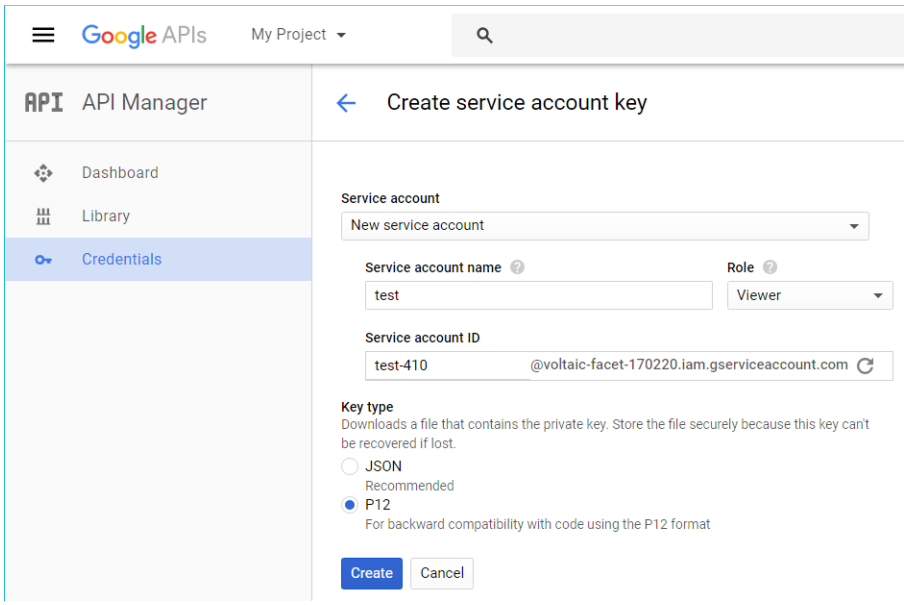
   b. Select your organization, if you see an organization dropdown list.
   c. Click the + button.
   d. In the *Project name* field, enter your project name, then click *Create*.
4. Enable the Admin SDK:
   a. Select your project from the toolbar list, then go to the *Library* tab.
   b. Under *G Suite APIs*, click *Admin SDK*.



c. Click *ENABLE*.

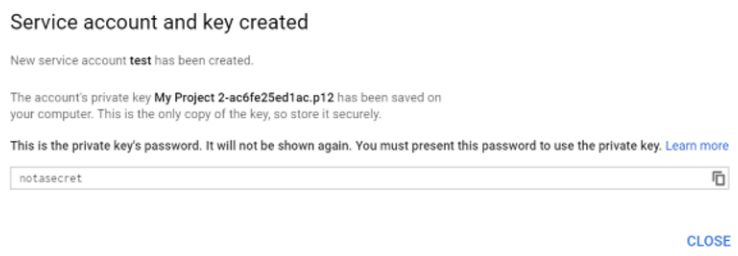


5. Create a service account:
   a. Go to the *Credentials* tab and select *Create Credentials* > *Service account key*.
   b. From the *Service account* list, select *New Service Account*. Enter a service account name.
   c. From the *Role* list, select *Project* > *Viewer*.
   d. Select *P12* as the *Key type* and click *Create*.

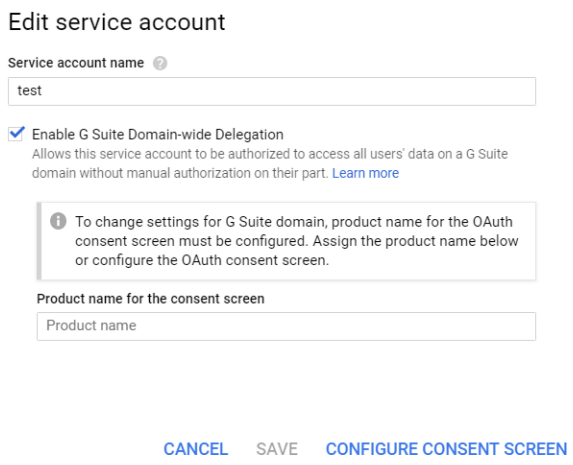


After you create the service account, a private key with the `P12` extension is saved on your computer.

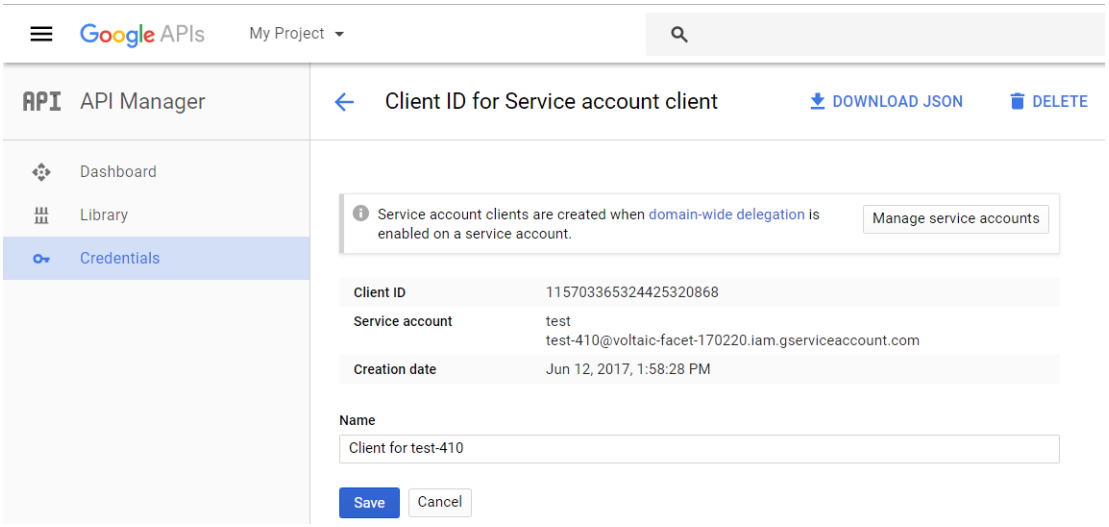
The private key with the `P12` extension is the only copy you will receive. Keep it in a safe place. You should also remember the password prompted on the screen. At this time, that password should be **`notasecret`**.



6. Go to the *Credentials* page > *Manage service accounts*.
7. *Edit* the service account you just created and select the *Enable Google Apps Domain-Wide Delegation* checkbox. Enter a *Product name for the consent screen* if this field appears.



8. Click *Save*.
9. Click *View Client ID* to see your service account information. Record the client ID, service account, and the associated private key (downloaded in step 5d).



To use the private key in EMS, it needs to be converted to `.pem` format. You can use the following `openssl` command to convert it. Remember to use the notasecret password.

```
C:\OpenSSL-Win64\bin>openssl pkcs12 -in demo-976b9d6e9328.p12 -out
     serviceAccount-demo.pem -nodes -nocerts
Enter Import Password:
```

Adding service account credentials to the Google Admin console

This section describes how to add the client ID from the service account credentials to the Google Admin console. These settings allow Google to trust FortiClient EMS, which enables FortiClient EMS to retrieve information from the Google domain.

To add the client ID:

1. In the Google Admin console, go to *Security* > *Advanced settings* > *(you may need to click "show more" to see this)* > *Manage API client access*.
2. Set the following options:
   a. For the *Client Name* option, add the client ID from the service account credentials.
   b. For the *API Scopes* option, add the following string:
   https://www.googleapis.com/auth/admin.directory.orgunit.readonly,https://www.googleapis.com/auth/admin.directory.user.readonly

   The API scopes are case-sensitive and must be lowercase. You may need to copy the string into a text editor and remove spaces created by words wrapping to the second line in the PDF.
3. Click *Authorize*.

Adding service account credentials to EMS

The section describes how to add the service account ID and service account certificate from the service account credentials to FortiClient EMS.

To add service account credentials:

1. In FortiClient EMS, go to *System Settings* > *EMS for Chromebook*.

   The default service account credentials display. Overwrite the default settings with the unique set of service account credentials received from Fortinet.
2. The *Service account* field shows the configured email address provided for the service account credentials. Click the *Update service account* button and configure the following information:

ID	Type a new email address for the service account credentials.

Private key	Click *Browse* and select the certificate provided with the service account credentials.

3. Click *Save*.
4. Update the client ID in the Google Admin console.

The service account credentials are a set. If you change one credential, you must change the other two credentials.

GUI

The FortiClient EMS GUI consists of the following areas:

- Banner on page 63
- Left pane on page 63
- Content pane on page 66

Banner

Option	Description
Download icon	Displays if a new version of FortiClient EMS is available on FDS.
Bell icon	Click the bell icon to display all alert logs.
<Logged in username>	Click the dropdown list beside the <logged in username> to log out of FortiClient EMS.

Left pane

The left navigation pane is used to display content in the right content pane.

Option		Description
Dashboard		
	FortiClient Status	Displays a dashboard of information about all managed endpoints.
	Vulnerability Scan	Displays the Current Vulnerabilities Summary chart that provides a centralized vulnerability summary for all managed endpoints. You can observe high-risk hosts and critical vulnerabilities existing on endpoints. You can also access links on how to fix or repair the vulnerabilities.
	Chromebook Status	Displays a dashboard of information about all managed Chromebooks. Only available if the *EMS for Chromebooks Settings* option is enabled in *System Settings* > *Server*.
Endpoints		
	All Endpoints	Manage all endpoints.

Option		Description
	Manage Domains	Add and manage AD domains.
	Domains	Manage endpoints from AD domains. You can also add an AD domain if none exist.
	Workgroups	Manage endpoints from workgroups.
Google Domains		Only available if the *EMS for Chromebooks Settings* option is enabled in *System Settings* > *Server*.
	All Users	Manage all users from Google domains.
	Manage Domains	Add and manage Google domains.
	Domains	Manage users from Google domains. You can also add a Google domain if none exist.
Quarantine Management		
	Files	View and whitelist files quarantined on endpoints by Sandbox Detection or Antivirus Protection.
	Whitelist	View and delete whitelisted files from the *Whitelist* pane.
Software Inventory		
	Applications	View applications installed on endpoints. Display applications by application or application vendor name.
	Hosts	View applications installed on endpoints, sorted by endpoint.
Endpoint Profiles		
	Manage Profiles	Create and assign profiles and manage profile updates for all profiles.
	Local Profiles	Create and assign profiles and manage profile updates for local Windows, Mac, and Linux profiles.
	Local Chromebook Profiles	Create and assign profiles and manage profile updates for local Chromebook profiles. Only available if the *EMS for Chromebooks Settings* option is enabled in *System Settings* > *Server*.
Endpoint Components		
	Manage Installers	Add and manage FortiClient installers.
	Manage FortiSandboxes	Add and manage FortiSandbox units.

Option		Description
	Manage CA Certificates	Import CA certificates into FortiClient EMS.
Gateway Lists		Create and assign gateway lists and manage list updates.
Administration		
	Administrators	Add and manage EMS administrators.
	User Server	Configure an AD domain as the user server. This is used to authenticate EMS administrators.
	User Settings	Configure the inactivity timeout.
	Group Assignment Rules	Configure rules to automatically place endpoints into custom groups based on their tag or IP address.
	Back up Database	Back up the FortiClient EMS database.
	Restore Database	Restore the FortiClient EMS database.
	Upgrade License	Upgrade or renew the FortiClient EMS license.
	Upgrade License for Chromebooks	Upgrade or renew the FortiClient EMS for Chromebooks license. Only available if the *EMS for Chromebooks Settings* option is enabled in *System Settings > Server*.
	Logs	View log messages generated by FortiClient EMS and download raw logs.
System Settings		
	Server	Change the IP address and port and configure other server settings for FortiClient EMS.
	Logs	Specify what level of log messages to capture in FortiClient EMS logs and when to automatically delete logs and alerts.
	FortiGuard	Configure FortiManager to use as override for FortiGuard updates.
	Endpoints	Configure endpoint settings.
	Login Banner	Enable the pre-login banner to display a message to a user logging into FortiClient EMS.
	EMS for Chromebooks	Configure settings specific to FortiClient EMS, including adding service account credentials and enabling Chromebook management.
	EMS Alerts	Enable alerts for FortiClient EMS events.

Option		Description
	Endpoint Alerts	Enable alerts for endpoint events.
	SMTP Server	Set up an SMTP server to enable email alerts.
	Custom Messages	Customize the message that displays on an endpoint when it has been quarantined by FortiClient EMS
Help		
	Getting Started	Provides access to links to the FortiClient EMS*Release Notes, QuickStart Guide*, and other resources.
	Technical Documentation	Link to the FortiClient EMS documentation.
	How-To Videos	Link to the Fortinet Video Library website.
	Forums	Link to Fortinet Customer Service and Support forum.
	Set up FortiClient EMS for Chromebooks	Link to an introductory video showing how to configure FortiClient EMS to manage Chromebooks.
	Introduction to FortiClient EMS	Link to an introductory video for FortiClient EMS, which gives an overview of features, modes, and system requirements for FortiClient EMS 1.0.
	How to License FortiClient EMS	Link to a video showing how to license or renew FortiClient EMS 1.0 with more endpoints.
	Adding a Domain to FortiClient EMS	Link to a video showing how to add an Active Directory domain to FortiClient EMS.
	Create Support Package	Create a support package to provide to the Fortinet technical support team for troubleshooting.
	FortiGuard	View list of engine and signature versions for this version of FortiClient EMS.

Content pane

The right content pane displays the user interface controls that correspond to the selection made in the left pane. The status and menu icons in the top-right display controls what you can use to configure additional settings for user management and each individual endpoint.

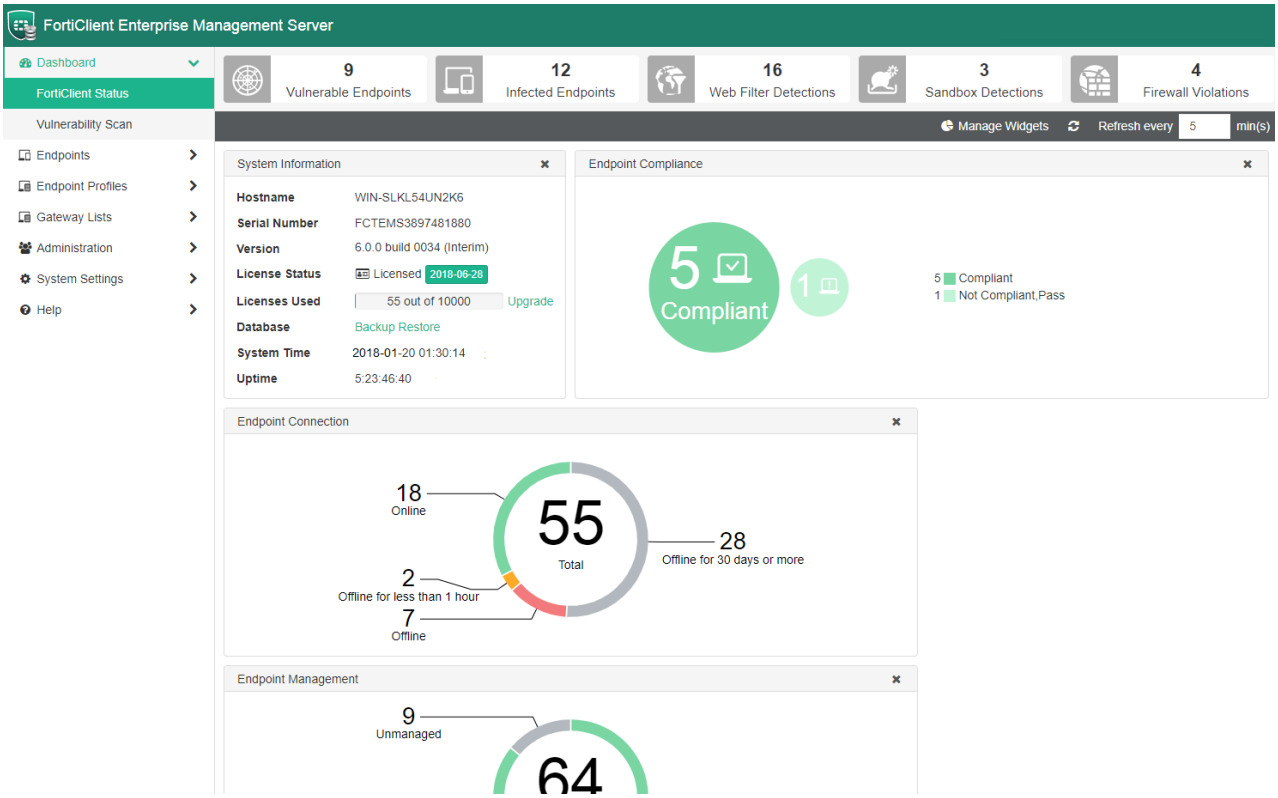
Dashboard

You can use the Dashboard to view summary information about the system and endpoints. You can view summary information about vulnerability scans on endpoints.

Viewing the FortiClient Status

To view the FortiClient Status:

1. In the left pane, click *Dashboard* > *FortiClient Status*.
   A *System Information* widget and charts and widgets of summary information display. See System Information widget on page 68 and FortiClient Status charts and widgets on page 68.



2. Click an event summary.
   The list of endpoints for the summary displays.
3. Click the *Back* button to return to the *FortiClient Status* pane.
4. Click a pie chart.
   The *Endpoints* content pane displays with more details about the endpoints related to the pie charts. See also Viewing the Endpoints content pane on page 78.

System Information widget

The following information displays in the *System Information* widget:

Option	Description
Hostname	Name of the computer on which FortiClient EMS is installed.
Serial Number	Serial number for FortiClient EMS.
Version	Version number for FortiClient EMS. Also displays the build number. If the current build is an interim build, also displays *(Interim)* beside the build number.
License Status	Status of the license for FortiClient EMS. Also displays a button for activating, upgrading, or renewing a license, depending on the license status. If you have just installed EMS, click *Activate* to upload your license file. If you have a non-expired license, but want to upgrade your license, click the *Upgrade* button to upgrade your license file. If your current license is expiring, the *Renew* button is enabled for you to upload your new license file. See License status on page 42.
Licenses Used	Number of licenses used out of the total number of available licenses.
Database	Options to back up and restore the database. Click *Backup* to back up the database. Click *Restore* to restore a backed up database.
System Time	Time and date used by the computer on which FortiClient EMS is installed.
Uptime	Number of days, hours, minutes, and seconds FortiClient EMS has been running.

FortiClient Status charts and widgets

FortiClient Status displays a number of pie charts. Each pie chart provides a summary of endpoint information. The sections in each chart are links. You can click any section of the pie charts or any row in the table to display more details.

Option	Description
Endpoint Charts	
Endpoint Activity	Shows a summary of endpoint activity information. Categories are: • FortiGate On-net • FortiGate Off-net • FortiGate Offline • FortiGate Not Registered • EMS On-net • EMS Off-net
Endpoint Alerts	Shows the number of endpoints with alerts, including pending software updates, out-of-date protection, and out-of-sync profiles.

Option	Description
Endpoint Compliance	Shows the number of endpoints that are: • Compliant • Not Compliant, Pass • Not Compliant, Blocked • Not Compliant, Warning
Endpoint Connection	Shows the number of endpoints that are: • Online • Offline for less than one hour • Offline • Offline for 30 days or more
Managed Mac FortiClient Versions	This chart indicates the percentage of macOS endpoints with each version of FortiClient installed. Sorting by version lists FortiClient versions from most recent to least recent. For example, FortiClient 6.0.0 is listed first, then FortiClient 5.6.6, FortiClient 5.6.5, and so on. Sorting by count lists FortiClient versions from the version with the largest number of endpoints to the version with the smallest number of endpoints. For example, if there are 600 endpoints with FortiClient 5.6.6 installed and 40 endpoints with FortiClient 6.0.0 installed, FortiClient 5.6.6 is listed first.
Managed Windows FortiClient Versions	This chart indicates the percentage of Windows endpoints with each version of FortiClient installed. You can sort the data by version or count. Sorting by version lists FortiClient versions from most recent to least recent. For example, FortiClient 6.0.0 is listed first, then FortiClient 5.6.6, FortiClient 5.6.5, and so on. Sorting by count lists FortiClient versions from the version with the largest number of endpoints to the version with the smallest number of endpoints. For example, if there are 600 endpoints with FortiClient 5.6.6 installed and 40 endpoints with FortiClient 6.0.0 installed, FortiClient 5.6.6 is listed first.
Managed Linux FortiClient Versions	This chart indicates the percentage of Linux endpoints with each version of FortiClient installed. You can sort the data by version or count.
Endpoint Management	This chart indicates how many endpoints are disconnected and connected.
Mac Operating Systems	This chart indicates the number of endpoints running each version of the macOS operating system. You can sort the data by version or count. Sorting by version lists macOS versions from most recent to least recent. For example, macOS 10.13 High Sierra is listed first, then macOS 10.12 Sierra, OS X 10.11 El Capitan, and so on. Sorting by count lists FortiClient versions from the version with the largest number of endpoints to the version with the smallest number of endpoints. For example, if there are 600 endpoints with macOS 10.12 Sierra installed and 40 endpoints with macOS 10.13 High Sierra installed, macOS 10.12 Sierra is listed first.

Option	Description
Windows Operating Systems	This chart indicates the number of endpoints running each version of the Windows operating system. You can sort the data by version or count. Sorting by version lists Windows versions from most recent to least recent. For example, Windows 10 is listed first, then Windows 8, Windows 7, and so on. Sorting by count lists FortiClient versions from the version with the largest number of endpoints to the version with the smallest number of endpoints. For example, if there are 600 endpoints with Windows 7 installed and 40 endpoints with Windows 10 installed, Windows 7 is listed first.
Linux Operating Systems	This chart indicates the number of endpoints running each version of the Linux operating system. You can sort the data by version or count. Sorting by version lists Linux versions from most recent to least recent. For example, Ubuntu 18.10 is listed first, then Ubuntu 17.10, Ubuntu 16.04, and so on. Sorting by count lists FortiClient versions from the version with the largest number of endpoints to the version with the smallest number of endpoints. For example, if there are 600 endpoints with Ubuntu 16.04 installed and 40 endpoints with Ubuntu 18.10 installed, Ubuntu 16.04 is listed first.
Endpoint Telemetry & Fabric	This chart indicates how many endpoints are connected to each FortiGate. It also indicates the number of endpoints not participating in the Security Fabric.
Top 3 Lists	
Antivirus Detection	This chart indicates the top three endpoints with antivirus alerts, including the number of antivrus alerts for each endpoint.
Sandbox Detection	This chart indicates the top three endpoints with FortiSandbox alerts, including the number of FortiSandbox alerts for each endpoint.
Vulnerability Detection	This chart indicates the top three endpoints with antivirus alerts, including the number of vulnerabilities detected for each endpoint.
Web Filter Detection	This chart indicates the top three endpoints with web filter alerts, including the number of web filter alerts for each endpoint.

Viewing the Vulnerability Scan dashboard

To view the Vulnerability Scan dashboard:

1. In the left pane, click *Dashboard* > *Vulnerability Scan*. Charts and widgets display a summary of vulnerability scan information.
2. Click a pie chart to view details about the vulnerabilities.

Vulnerability Scan charts and widgets

The *Vulnerability Scan* dashboard displays a number of pie charts. Each pie chart provides a summary of endpoint information. The sections in each chart are links. You can click any section of the pie charts or any row in the table to

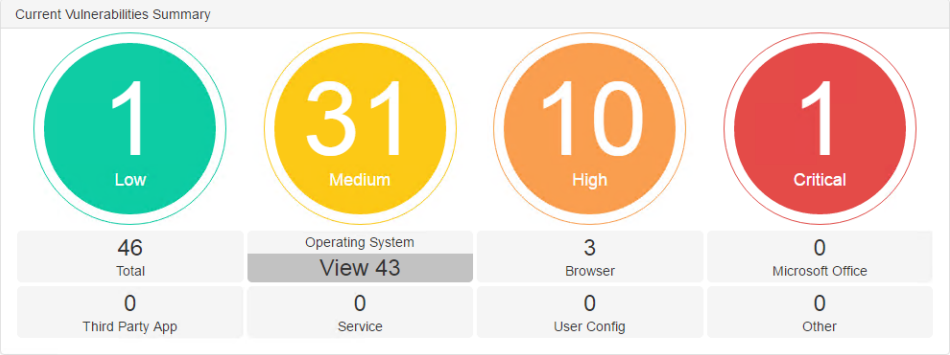
display more details.

Option	Description
Current Vulnerabilities Summary	Displays the following summaries of current vulnerabilities: • Total (total number of vulnerabilities) • Operating System (number of operating system vulnerabilities) • Browser (number of browser vulnerabilities) • Microsoft Office (number of Microsoft Office vulnerabilities) • Third Party App (number of third-party application vulnerabilities) • Service (number of service vulnerabilities) • User Config (number of user configuration vulnerabilities) • Other (number of other vulnerabilities that do not fit any of the above categories) When you click a vulnerability tile, the severity of vulnerabilities displays in the colored circles above.
Endpoint Scan Status	Displays the following summaries about endpoints: • Vulnerable Endpoints • Un-Scanned Endpoints • Secured Endpoints • Scanning Endpoints
Top 10 Vulnerable Endpoints	Displays the top ten vulnerable endpoints and the number of vulnerabilities within that endpoint.
Top 10 Vulnerabilities	Displays the top ten vulnerabilities.

Viewing current vulnerabilities

To view current vulnerabilities:

1. Click a vulnerability tile.
2. The colored circles change and display the number of vulnerabilities and severities corresponding to the selected *Vulnerability Tile*.

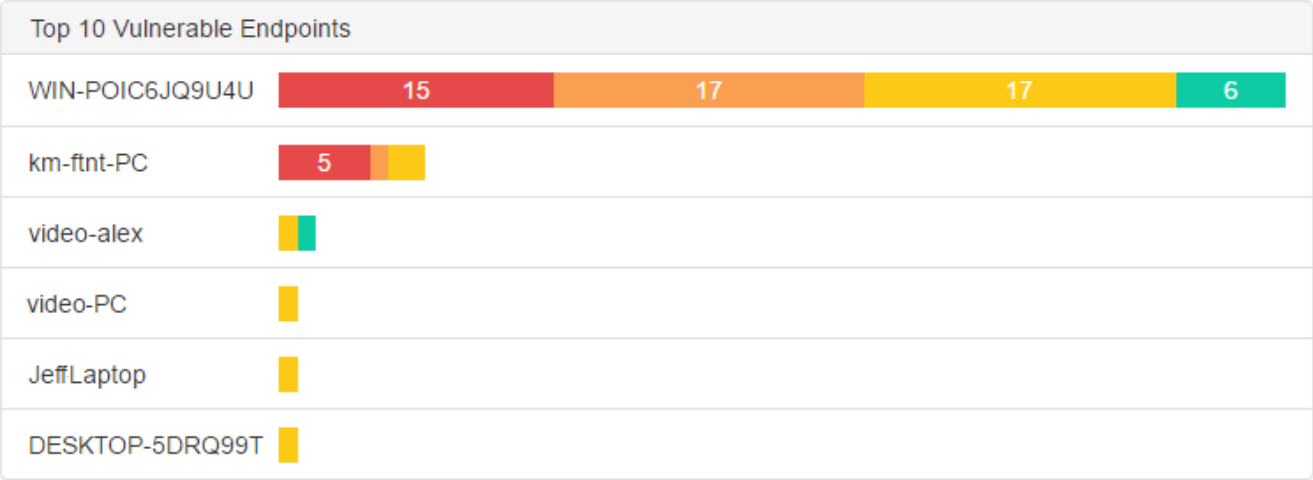


For example, click the *Operating System* tile, which has a total of 46 *Vulnerabilities*. The *Vulnerabilities* are organized by *Severity*:

- 1/62 is *Low Risk* (green circle)
- 31/62 are *Medium Risk* (yellow circle)
- 10/62 are *High Risk* (orange circle)
- 1/62 is *Critical Risk* (red circle)

Viewing top ten vulnerabilities on endpoints

How to read the Top 10 Vulnerable Endpoints widget:



For example, the *Top 10 Vulnerable Endpoints* vulnerabilities displays. The *Vulnerabilities* are shown in a segmented bar graph and organized by severity:

WIN-POIC6JQ9U4U has the following:

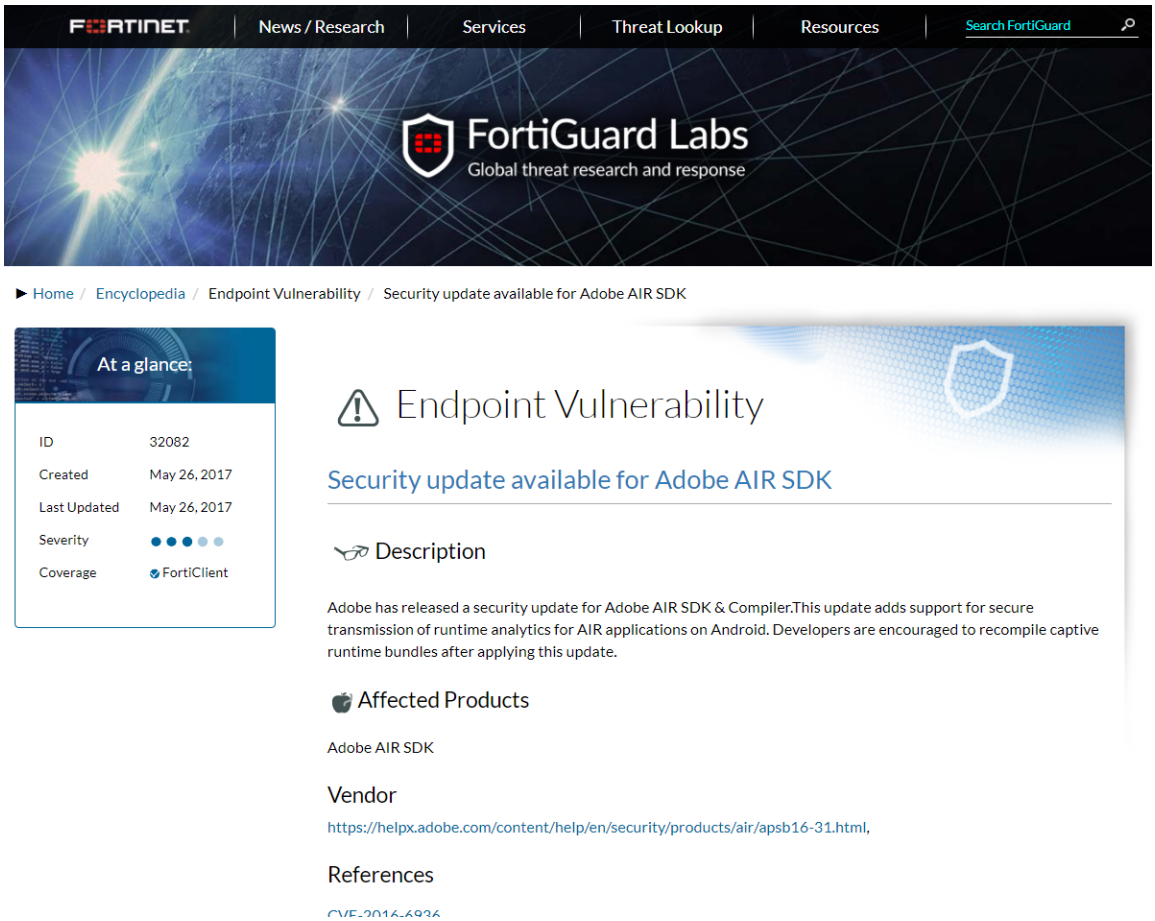
- 15 *Critical Vulnerabilities* (red bar)
- 17 *High Risk Vulnerabilities* (orange bar)
- 17 *Medium Risk Vulnerabilities* (yellow bar)
- 6 *Low Risk Vulnerabilities* (green bar)

How to read the Top 10 Vulnerabilities widget:

Top 10 Vulnerabilities	
Cumulative Security Update for Internet Explorer	1 Host
Cumulative Security Update for Microsoft Edge	1 Host
Microsoft Security Bulletin MS16-120: Security Update for Microsoft Graphics Component	1 Host
Security Update for Group Policy	1 Host
Security Update for Microsoft Graphics Component	1 Host
Security Update for Microsoft RPC	1 Host
Security Update for Microsoft Video Control	1 Host
Security Update for Microsoft Windows to Address Remote Code Execution	1 Host
Security Update for Microsoft XML Core Services	1 Host
Security Update for Netlogon	1 Host

The *Top 10 Vulnerabilities* widget displays the type of vulnerability and how many hosts have the vulnerability. For example, the *Cumulative Security Update for Internet Explorer Vulnerability* has one host affected.

When you click a vulnerability, you are redirected to the *FortiGuard Labs Threat Encyclopedia* where details about the vulnerability are available.



Viewing Chromebook Status

Chromebook Status displays a number of pie charts. Each pie chart provides a summary of Chromebook information. The sections in each chart are links. You can click any section of the pie charts or any row in the table to display more details. Chromebook Status is only available if *EMS for Chromebooks Settings* is selected in *System Settings > Server*.

Option	Description
User Charts	
Active Users	This chart displays the active and inactive users.
Managed Users	This chart displays the managed and unmanaged users.
Webfilter Charts	
Top 10 Violations by Category	The chart displays the top ten web filter violations by category in the past few days. You can configure the number of days. Go to *System Settings > Logs*.

Option	Description
Top 10 Violations by User	The chart displays the top web filter violations by user in the past few days. You can configure the number of days. Go to *System Settings* > *Logs*.
Others	
System Information	This widget displays summary information for the system.

Endpoint Management

FortiClient EMS needs to determine which devices to manage. For Windows, Mac, and Linux endpoints, device information can come from an Active Directory server, Windows workgroup, or manual FortiClient connection.

For Chromebooks, device information comes from the Google Admin console.

Windows, Mac, and Linux endpoints

Device information can come from an Active Directory server, Windows workgroup, or manual FortiClient connection. You can create groups to organize endpoints.

Creating groups

You can create groups to organize endpoints. You can also rename and delete groups.

To create groups:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup and select *Create group*. The *Create group* dialog box displays.
3. In the *Required* box, type a name for the group, and click *Confirm*.
   The group is created.

To rename groups:

1. Go to *Endpoints*.
2. Right-click the group, and select *Rename group*. The *Rename the group* dialog box displays.
3. In the *Required* box, type the new name, and click *Confirm*.
   The group is renamed.

To delete groups:

1. Go to *Endpoints*.
2. Right-click the group, and select *Delete group*. A confirmation dialog box displays.
3. Click *Yes*.
   The group and any subgroups are deleted.

Adding endpoints

You can add endpoints using an Active Directory service. Endpoints are also added when endpoint users manually connect FortiClient Telemetry to FortiClient EMS.

Adding endpoints using an Active Directory domain server

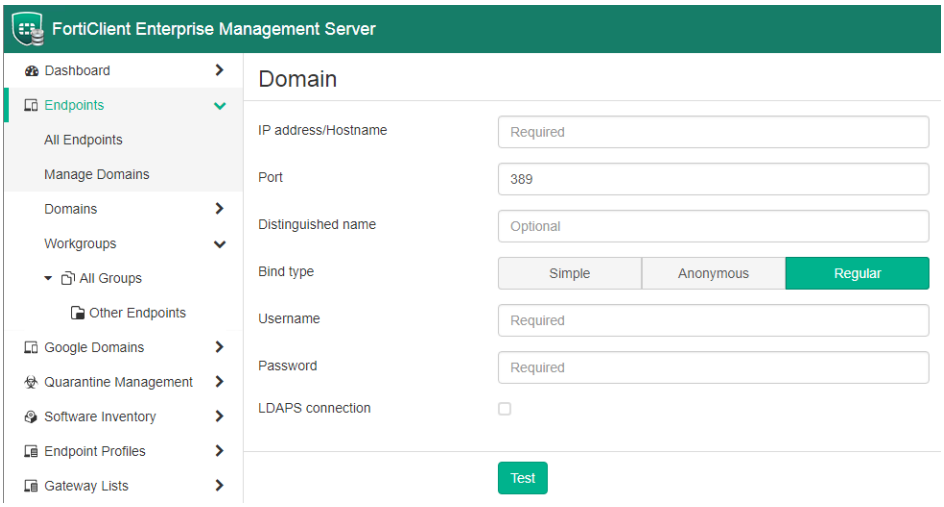
Endpoints can be manually imported from an Active Directory (AD) domain server. You can import and synchronize information about computer accounts with an LDAP or LDAPS service. You can add endpoints by identifying endpoints that are part of an AD domain server.

An instructional video on how to add a domain is available in the Fortinet Video Library.

You can add the entire domain or an organizational unit (OU) from the domain.

To add endpoints using an Active Directory domain service:

1. Click *Endpoints* > *Manage Domains* > *Add*. The *Domain* pane displays.



2. Configure the following options:

IP address/Hostname	Type the IP address or name.
Port	Type the port number.
Distinguished name	Type the distinguished name (optional).
Bind type	Select the bind type: *Simple*, *Anonymous*, or *Regular*. When you select *Regular*, enter the *User DN* and *Password*.
Username	Available when *Bind Type* is set to *Regular*. Type the user DN.
Password	Available when *Bind Type* is set to *Regular*. Type the user password.

Show Password	Available when *Bind Type* is set to *Regular*. Turn on and off to show or hide the password.
LDAPS connection	Turn on to enable a secure connection protocol when *Bind Type* is set to *Regular*.

3. Click *Test* to test the domain settings connection.
4. If the test is successful, select *Save* to save the new domain. If not, correct the information as required then test the settings again.

Connecting manually from FortiClient

Endpoint users can manually connect FortiClient Telemetry to FortiClient EMS by specifying the IP address for FortiClient EMS in FortiClient Console. This process is sometimes called registering FortiClient to FortiClient EMS. AWS

To connect FortiClient Telemetry to FortiClient EMS:

1. In FortiClient Console on the endpoint, go to the *Compliance & Telemetry* tab.
2. In the *FortiGate or EMS IP* box, type the EMS IP address, and click *Connect*.

   FortiClient connects to FortiClient EMS.

For information about FortiClient, see the *FortiClient Administration Guide* available on docs.fortinet.com/forticlient/admin-guides.

The FortiClient Telemetry gateway port may be appended to the gateway list address on FortiClient and separated by a colon. When the port is not provided, FortiClient attempts to connect to the IP address given using the default port. The default connection port in FortiClient 5.2 is 8010 and in FortiClient 5.4 is 8013. By default, FortiClient EMS listens for connection on port 8013.

Note it is considered best practice to add endpoints using the method in Adding endpoints using an Active Directory domain server on page 77. Connecting FortiClient to FortiClient EMS manually is only recommended for troubleshooting purposes.

Viewing endpoints

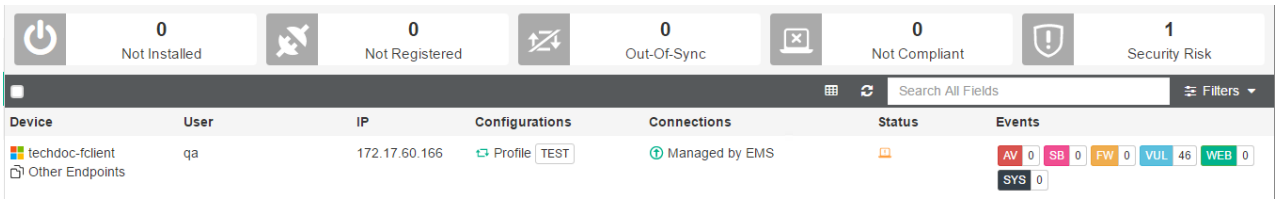
After you add endpoints to FortiClient EMS, you can view the list of endpoints in a domain or workgroup in the *Endpoints* pane. You can also view details about each endpoint in the *Client Details* pane and use filters to access endpoints with specific qualities.

Viewing the Endpoints content pane

You can view information about endpoints on the *Endpoints* content pane.

To view the Endpoints content pane:

1. Go to *Endpoints*, and select *All Endpoints*, a domain, or workgroup.
   The list of endpoints in FortiClient EMS, a quick status bar, and a toolbar display in the content pane.



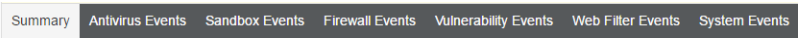
Not Installed	Number of endpoints that do not have FortiClient installed. Click to display the list of endpoints without FortiClient installed.
Not Registered	Number of endpoints not connected to FortiClient EMS or FortiGate. Click to display the list of disconnected endpoints.
Out-Of-Sync	Number of endpoints with an out-of-sync profile. Click to display the list of endpoints with out-of-sync profiles.
Not Compliant	Number of endpoints not compliant with the FortiGate compliance rules. Click to display the list of not compliant endpoints.
Security Risk	Number of endpoints that are a security risk. Click to display the list of endpoints.
Checkbox	Click to select all endpoints displayed in the content pane.
Show/Hide Heading	Click to hide or display the following column headings: *Device*, *User*, *IP*, *Configurations*, *Connections*, *Status*, and *Events*.
Show/Hide Full Group Path	Click to hide or display the full path for the group that the endpoint belongs to.
Refresh	Click to refresh the list of endpoints in the content pane.
Search All Fields	Type a value and press *Enter* to search for the value in the list of endpoints.
Filters	Click to display and hide filters you can use to filter the list of endpoints.
Device	Visible when headings are displayed. Displays an icon to represent the operating system on the endpoint and the device name.
User	Visible when headings are displayed. Displays the name of the user logged into the endpoint.
IP	Visible when headings are displayed. Displays the endpoint's IP address.
Configurations	Visible when headings are displayed. Displays the name of the profile assigned to the endpoint and the profile's synchronization status.
Connections	Visible when headings are displayed. Displays whether the endpoint is connected to FortiClient EMS or FortiGate and the connection status of *Online*, *Offline*, or *Not Registered*.

Status	Visible when headings are displayed. Displays one of the following compliance statuses for the endpoint. • Compliant • Not compliant • Not participating in compliance • Quarantined • Excluded • Not registered • Not installed
Events	Visible when headings are displayed. Displays FortiClient events for the endpoint.

2. Click an endpoint to display its details in the content pane.
The following dropdown lists display in the toolbar for the selected endpoint:

Checkbox	Click to select and deselect all endpoints in the content pane. You can then select or clear the checkbox for individual endpoints to fine-tune the list of selected endpoints.
Scan	Click to start a Vulnerability or AntiVirus scan on the selected endpoint.
Patch	Click to patch all critical and high vulnerabilities on the selected endpoint. Choose one of the following options: • Selected Vulnerabilities on Selected Clients • Selected Vulnerabilities on All Affected Clients • All Critical and High Vulnerabilities
Action	Click to perform one of the following actions on the selected endpoint: • Upload FortiClient Logs • Request Diagnostic Results • Update Signatures • Re-register • De-register • Register • Quarantine • Un-quarantine • Exclude from Management • Mark as Uninstalled • Delete Device

The following tabs are available in the content pane toolbar when you select an endpoint:



Summary	

	<user name>	Displays the name of the user logged into the selected endpoint. Also displays the user's avatar, email address, and phone number if these are provided to FortiClient on the endpoint. If the user's LinkedIn, Google, Salesforce, or other cloud app account is linked in FortiClient, the username from the cloud application displays.
	Device	Displays the selected endpoint's device name.
	OS	Displays the selected endpoint's operating system and version number.
	IP	Displays the selected endpoint's IP address.
	MAC	Displays the selected endpoint's MAC address.
	Last Seen	Displays the last date and time that FortiClient sent a keep-alive message to EMS. This information is useful if FortiClient is offline because it indicates when the last keep-alive message occurred.
	Location	Displays whether the selected endpoint is onnet or offnet.
	Connection	Displays when the selected endpoint is connected to FortiClient EMS or FortiGate. Also displays the connection status.
	Configuration	Displays the following information for the selected endpoint: • Profile: Name of the profile assigned to the selected endpoint • Installer: Name of the FortiClient installer used for the selected endpoint. Displays *Not Assigned* if no FortiClient installer has been assigned to the selected endpoint. • Gateway List: Name of the gateway list used for the selected endpoint. Displays *Not Assigned* if no gateway list has been assigned to the selected endpoint. • FortiClient Version: FortiClient version installed on the selected endpoint. • FortiClient Serial Number: Serial number for the selected endpoint's FortiClient license.
	Compliance	Displays if the endpoint is compliant. If the endpoint is not compliant, displays the features for which FortiClient is not compliant.
	Features	Displays which features are enabled for FortiClient.
Antivirus Events		
	Date/Time	Displays the antivirus event's date and time.
	Message	Displays the antivirus event's message.
Sandbox Events		
	Date/Time	Displays the sandbox event's date and time.
	Message	Displays the sandbox event's message.

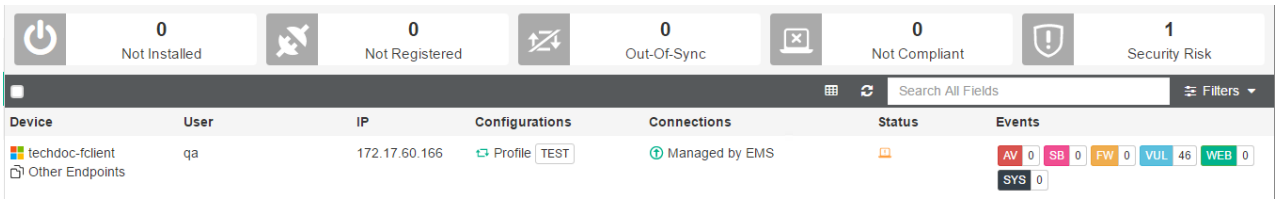
Firewall Events		
	Date/Time	Displays the firewall event's date and time.
	Message	Displays the firewall event's message.
Vulnerability Events		
	Vulnerability	Displays the vulnerability's name. For example, *Security update available for Adobe Reader*.
	Category	Displays the vulnerability's category. For example, *Third Party App*.
	Application	Displays the name of the application with the vulnerability.
	Severity	Displays the vulnerability's severity.
	FortiGuard ID	Displays the FortiGuard ID number. If you click the FortiGuard ID number, it redirects you to FortiGuard where further information is provided if available.
	Bulletin	Displays a link to a bulletin about the software vulnerability.
Web Filter Events		
	Date/Time	Displays the web filter event's date and time.
	Message	Displays the web filter event's message.
System Events		
	Date/Time	Displays the system event's date and time.
	Message	Displays the system event's message.

Using the quick status bar

You can use the quick status bar to quickly display filtered lists of endpoints on the *Endpoints* content pane.

To use the quick status bar:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup.
   The list of endpoints and quick status bar display.



3. Click one of the following buttons in the quick status bar:
   - Not Installed
   - Not Registered
   - Out-Of-Sync

- Not Compliant
- Security Risk

The list of affected endpoints displays.

4. Click an endpoint to display its details.
5. In the *Events* column, click the *AV <number>, SB <number>, FW <number>*, *VUL<number>*, *WEB <number>* and *SYS<number>* buttons to display the associated tab of details for the selected endpont.
6. Click the *Total* button to clear the filters.

   The unfiltered list of endpoints displays.

Viewing endpoint details

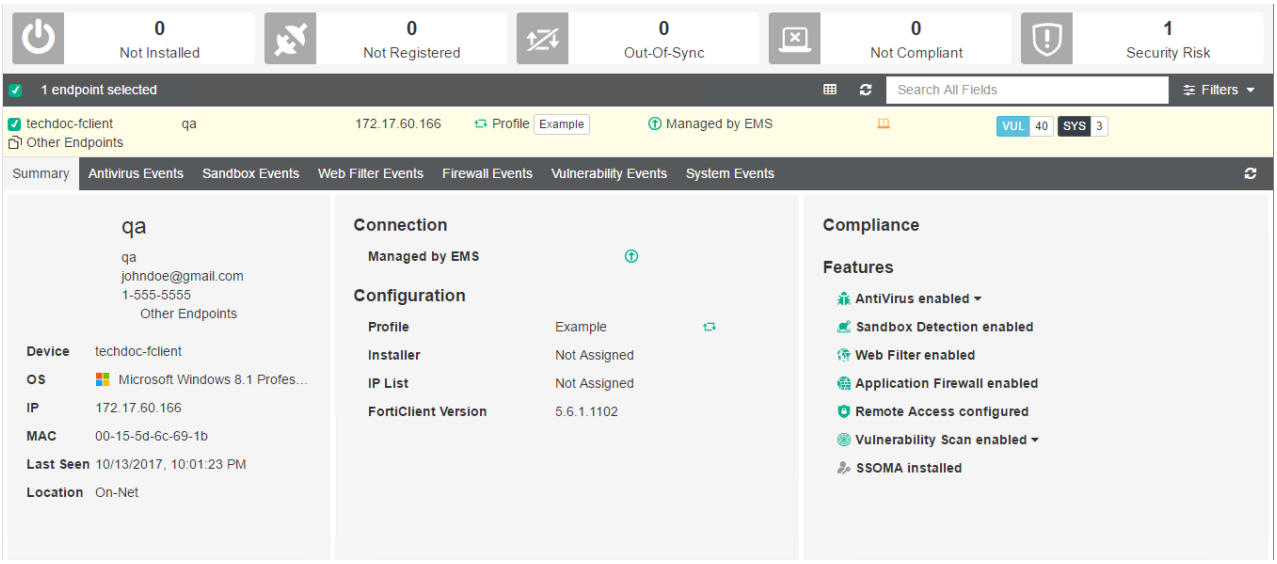
You can view each endpoint's details on the *Endpoints* content pane. For a description of the options on the *Endpoints* content pane, see Viewing the Endpoints content pane on page 78.

To view endpoint details:

1. Go to *Endpoints*, and select *All Domains*, a domain, or workgroup.

   The list of endpoints for the selected domain or workgroup displays.
2. Click an endpoint to display details about it in the content pane.

   Details about the endpoint display in the content pane.



Filtering the list of endpoints

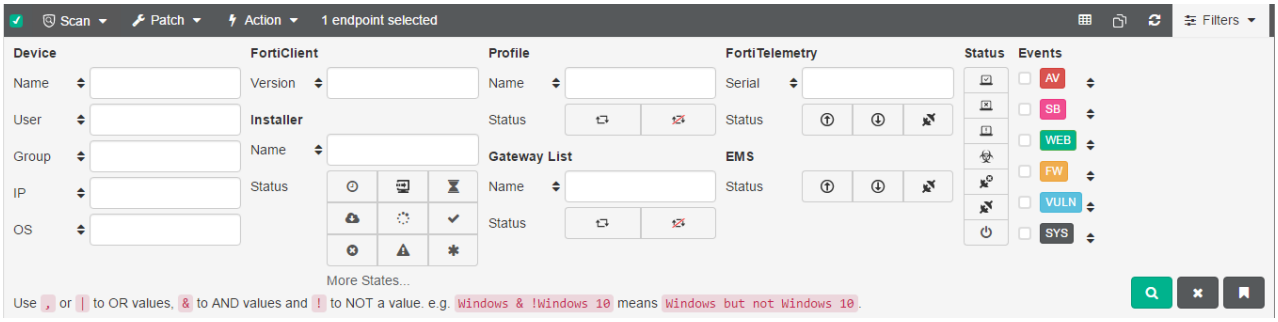
You can filter the list of endpoints displayed on the *Endpoints* content pane.

To filter endpoints:

1. Go to *Endpoints*.
2. Click *All Domains*, a domain, or workgroup.

   The list of endpoints displays.

3. Click the *Filters* menu, and set filters.
   The filter options display.
   For text values, you can use a comma (,) to separate values and an exclamation mark (!) to exclude a value.
   For buttons, hover the mouse over each button to view its tooltip.



Device		Lists the filter options for devices.
	Name	Type the name(s) to include in the filter. You can exclude a name or names from the filter using an exclamation mark (!).
	User	Type the name of the user(s) to include in the filter. You can exclude a name or names from the filter using an exclamation mark (!).
	Group	Type the name of the group(s) to include in the filter. You can also exclude a name or names from the filter using an exclamation mark (!).
	IP	Type the IP address to include in the filter. You can exclude an IP address from the filter using an exclamation mark (!).
	OS	Type the name of the operating system(s) to include in the filter. You can exclude a name or names from the filter using an exclamation mark (!).
FortiClient		Lists the filter options for FortiClient version numbers.
	Version	Enter the FortiClient version number to include in the filter. You can exclude a version or versions from the filter using an exclamation mark (!).
Installer		Lists the filter options for deployment.
	Name	Type the name(s) of the installer to include in the filter. You can exclude a name or names from the filter using an exclamation mark (!).
	Status	Click one or more deployment status buttons to include in the filter. Selected status buttons are green. Hover the mouse over each button to view its tooltip. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
	More States	Click to display additional statuses to include in the filter.
Profile		

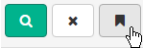
	Name	Type the name(s) of the profile to include in the filter. You can also exclude a name or names from the filter by using an exclamation mark (!).
	Status	Click the profile status to include in the filter. Selected status buttons are green. Choose between *Synced* and *Out-Of-Sync*. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
Gateway List		
	Name	Type the name(s) of the gateway IP list to include in the filter. You can also exclude a name or names from the filter by using an exclamation mark (!).
	Status	Click the gateway IP list status to include in the filter. Selected status buttons are green. Choose between *Synced* and *Out-Of-Sync*. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
FortiTelemetry		
	Serial	Select the FortiGate serial number to include in the filter.
	Status	Click the status for FortiClient Telemetry connection to FortiGate to include in the filter. Choose between *Online*, *Offline*, and *Not Registered*.
EMS		
	Status	Click the status for FortiClient Telemetry connection to EMS to include in the filter. Selected status buttons are green. Choose between *Online*, *Offline*, and *Not Registered*. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
Status		Click the compliance status to include in the filter. Selected status buttons are green. Choose between *Compliant*, *Not Compliant*, *Not Participating*, *Quarantined*, *Excluded*, *Not Registered*, *Not Installed*. Clear the status button to exclude the status from the filter. Excluded status buttons are gray.
Events		Select the events to include in the filter. The selected checkboxes beside the events are included in the filter. Clear the checkbox beside the event to exclude the event from the filter.
Bookmarks		Displays the list of saved filter settings. Displays only after you have saved a bookmark. Click the *Bookmark* button to name and save filter settings. Click a bookmark to use the saved settings. Click the *x* beside a bookmark to delete it.
Search		Click the *Search* button to apply the filter setting.
Reset		Click the *Reset* button to clear the filter settings.
Bookmark		Click the *Bookmark* button to save the filter settings as a bookmark.

4. Click *Search*.
   The filtered list of endpoints displays.
5. Click *Reset* to clear the filter settings.

Using bookmarks to filter the list of endpoints

You can save filter settings as bookmarks, then select the bookmarks to use them.

To create bookmarks to filter endpoints:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup.
   The list of endpoints displays.
3. Click the *Filters* menu, and set filters.
4. Click the *Bookmark* button.
   
   The *New Bookmark* box displays.
5. In the *New Bookmark* box, type a name for the filter settings, and press *Enter*.
   The bookmark displays under *Bookmarks*.

To use bookmarks to filter the list of endpoints:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup.
   The list of endpoints displays.
3. Click the *Filters* menu.
4. In the *Bookmarks* list, click a bookmark.
   The bookmark settings are used to filter the list of endpoints.

Managing endpoints

You can manage endpoints from the *Endpoints* pane.

Running AntiVirus scans on endpoints

You can run a full or quick AntiVirus scan on endpoints. Scanning starts on the endpoints with the next FortiClient Telemetry communication.

To run AntiVirus scans on endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Start full antivirus scan* or *Start quick antivirus scan*.

To run AntiVirus scans on an endpoint:

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup.
3. The list of endpoints displays in the content pane.
4. Click an endpoint, and from the *Scan* menu, select *Quick AV Scan* or *Full AV Scan*.

Running vulnerability scans on endpoints

You can run a vulnerability scan on endpoints. You can view the history of vulnerability scans for each endpoint on the *Client Details* pane.

To run vulnerability scans on endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Start vulnerability scan*.
   Vulnerability scanning starts on the endpoints with the next FortiClient Telemetry communication.

To run vulnerability scans on an endpoint:

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup.
   The list of endpoints displays in the content pane.
3. Click an endpoint, and from the *Scan* menu, select *Vulnerability Scan*.
   Vulnerability scanning starts on the endpoint with the next FortiClient Telemetry communication.

Patching vulnerabilities on endpoints

You can request FortiClient patch detected critical and high vulnerabilities on endpoints.

FortiClient can automatically patch many software. However, the endpoint user must manually patch some detected software vulnerabilities. If a vulnerability requires the endpoint user to download and install software to patch a vulnerability, FortiClient Console displays the information.

To patch vulnerabilities on endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Patch critical/high vulnerabilities*.
   FortiClient initiates automatic vulnerability patching with the next FortiClient Telemetry communication.

To patch vulnerabilities on an endpoint:

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup.
   The list of endpoints displays in the content pane.

3. Click an endpoint, and from the *Patch* menu, select one of the following options:
   - *Selected Vulnerabilities on Selected Clients*
   - *Selected Vulnerabilities on All Affected Clients*
   - *All Critical and High Vulnerabilities*

   FortiClient initiates automatic vulnerability patching with the next FortiClient Telemetry communication.

Uploading FortiClient logs

You can upload a FortiClient log file from one or several endpoints to FortiClient EMS. The log file is uploaded to the hard drive on the computer on which you are running EMS. The uploaded log file is not visible in the FortiClient EMS GUI.

To upload FortiClient logs:

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup.
   The list of endpoints displays in the content pane.
3. Click one or multiple endpoints, and from the *Action* menu, select *Upload FortiClient logs*.
   The `<number>_log` file is uploaded to the following location on your computer: `<drive>\Program Files (x86)\Fortinet\FortiClientEMS\logs`

Running the FortiClient diagnostic tool

You can use EMS to run the FortiClient Diagnostic Tool on one or multiple endpoints and export the results to the hard drive on the computer on which you are running FortiClient EMS. The exported information is not visible in the FortiClient EMS GUI.

To run the FortiClient diagnostic tool:

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup.
   The list of endpoints displays in the content pane.
3. Click one or multiple endpoints, and from the *Action* menu, select *Request Diagnostic Results*.
   The `<number>_Diagnostic_Result` file is uploaded to the following location on your computer: `<drive>:\Program Files (x86)\Fortinet\FortiClientEMS\logs`.

Updating signatures

You can use EMS to request FortiClient update signatures on the endpoints.

To update signatures:

1. Go to *Endpoints*.
2. Select *All Endpoints*, a domain, or workgroup.
   The list of endpoints displays in the content pane.

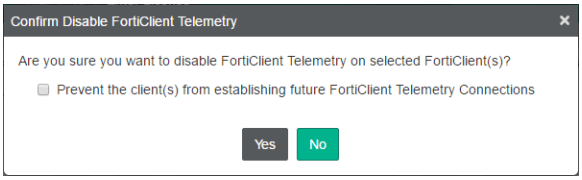
3. Click an endpoint, and from the *Action* menu, select *Update Signatures*.
   FortiClient receives the request to update signatures and downloads the signatures from the Internet.

Disconnecting and connecting endpoints

You can manually disconnect and connect endpoints using EMS.

To disconnect endpoints:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup. A list of endpoints displays.
3. Click an endpoint, and from the *Action* menu, select *Deregister*.
   A confirmation dialog box displays.



   You can prevent the endpoint from connecting in the future by selecting the *Prevent the client(s) from establishing future FortiClient Telemetry Connections* checkbox.
4. Click *Yes* to confirm.
   The endpoint is disconnected with the next FortiClient Telemetry communication.

To connect endpoints:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup. A list of endpoints displays.
3. Click an endpoint, and from the *Action* menu, select *Register*.
   The endpoint is connected with the next FortiClient Telemetry communication.

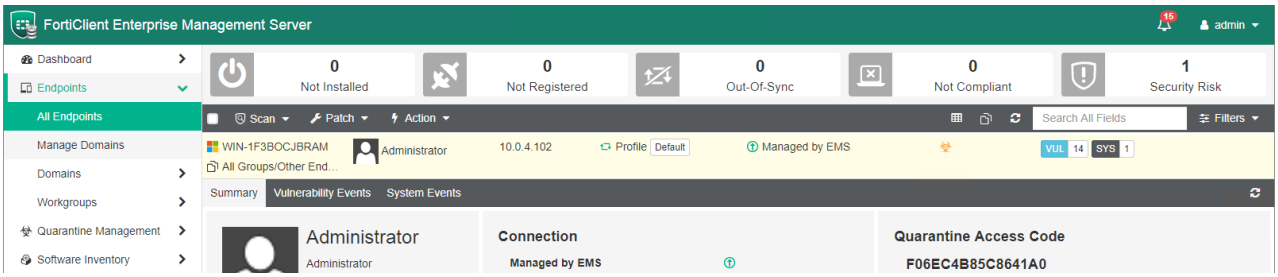
Quarantining endpoints

You can quarantine an endpoint using EMS. Quarantined endpoints cannot access the network.

To quarantine an endpoint:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup. A list of endpoints displays.
3. Click an endpoint, and from the *Action* menu, select *Quarantine*.
   The endpoint status changes to *Quarantined*, and the endpoint is quarantined with the next FortiClient Telemetry communication.
   You can remove an endpoint from quarantine by right-clicking the endpoint and selecting *Unquarantine*. The endpoint is removed from quarantine with the next FortiClient Telemetry communication and network access is restored.

Note you can also provide the endpoint user with a one-time access code. The user can enter the code to access FortiClient on a quarantined endpoint, then remove the endpoint from quarantine in the FortiClient console. The code is available under Quarantine Access Code after selecting a quarantined endpoint as seen below.



Quarantining an endpoint from FortiOS using EMS

In FortiOS 6.0, an administrator can quarantine FortiClient endpoints using EMS by enabling the *Quarantine FortiClient via EMS* option. The following lists the requirements for this feature:

- The FortiClient endpoint is connected to FortiGate and managed by EMS
- The FortiClient endpoint and FortiGate use the same FortiAnalyzer
- The EMS server managing the FortiClient endpoint is configured on the FortiGate. See the *FortiOS Handbook* for details on the FortiGate configuration required.

If *Quarantine FortiClient via EMS* is enabled, the following occurs when an indicator of compromise (IOC) is detected on an endpoint in the Security Fabric:

1. An IOC is detected on an endpoint.
2. FortiAnalyzer sends the endpoint information to FortiOS.
3. FortiOS sends the endpoint information to EMS.
4. EMS identifies and quarantines the endpoint.

Excluding endpoints from management

You can exclude endpoints from management.

To exclude endpoints from management:

1. Right-click a domain or workgroup.
2. Select *Exclude from management*.
   The domain or workgroup is excluded from management.

To exclude an endpoint from management:

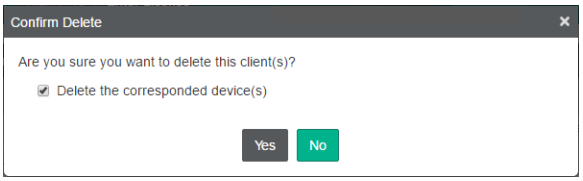
1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup. A list of endpoints displays.
3. Click an endpoint, and from the *Action* menu, select *Exclude from Management*.
   The endpoint is excluded from management.

Deleting endpoints

You can delete disconnected endpoints from EMS.

To delete endpoints:

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup. A list of endpoints displays.
3. If the endpoint has a status of *Registered*, disconnect the endpoint.
4. Click an endpoint, and from the *Action* menu, select *Delete Device*.
   A confirmation dialog box displays.



5. Click *Yes*.
   The endpoint is deleted from FortiClient EMS.

Provisioning FortiClient Android endpoints for central management

You can use a third-party QR code generator to create a QR code to distribute to FortiClient (Android) users. FortiClient (Android) users can scan the QR code from their device to automatically enable FortiTelemetry and attempt connection to the specified FortiClient EMS server and FortiGate.

QR codes can contain the FortiClient EMS server's hostname or IP address, port number, and a connection key. Only the FortiClient EMS hostname/IP address is required; all other fields are optional. The following table summarizes the possible syntax used to generate the QR code:

Scenario	Format	Example
Includes hostname or IP address, port number, and connection key.	fortitelemetry://<EMS hostname or IP address>:<port number> <connection key>	fortitelemetry://192.168.128.12:8013 11111
Includes hostname or IP address, port number, with no connection key.	fortitelemetry://<EMS hostname or IP address>:<port number>	fortitelemetry://192.168.128.12:8013
Includes hostname or IP address only. Uses the default port and has no connection key.	fortitelemetry://<EMS hostname or IP address>:	fortitelemetry://192.168.128.12:

1. Open the QR code generator of your choice.
2. Enter the hostname/IP address, port number, and/or connection key information as desired, using one of the formats above.
3. Generate the plain text QR code.
4. Email the QR code to FortiClient (Android) users.

For instructions on scanning the QR code from an Android device, see the *FortiClient (Android) 5.4 User Guide*.

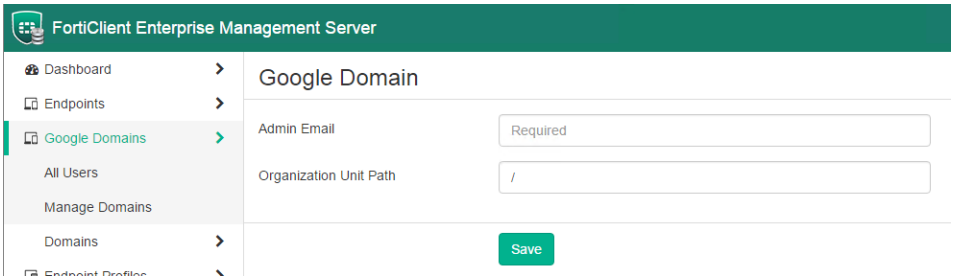
Google Domains

FortiClient EMS needs to determine which devices to manage. Device information comes from the Google Admin console. *Google Domains* is only available if *EMS for Chromebooks Settings* is selected in *System Settings* > *Server*. Note this section is only applicable if you are using FortiClient EMS to manage Google Chromebooks.

Adding Google domains

To add Google domains:

1. Go to *Google Domains* > *Manage Domains*, and click the *Add* button. The *Google Domain* pane displays.



2. In the *Admin Email* box, type your Google domain admin email.
3. In the *Organization Unit Path* box, type the domain organization unit path.

> / stands for the root of the domain.

4. Click *Save*.
   The Google domain information and users are imported into FortiClient EMS.

Viewing domains

After you add domains to FortiClient EMS, you can view the list of domains in *Google Domains*. You can also view the list of Google users in each domain and details about each Google user in the *User Details*, *Client Statistics*, and *Blocked Sites* panes.

Viewing the Google Users pane

You can view Google users' information in FortiClient EMS.

To view the Google Users pane:

1. Go to *Google Domains* > *Domains* and click a domain. The list of Google users displays.

Google Users Clear Filters

Name	Email	Last Login	Last Policy Retr	Domain	Organization Path
Art3 Sikes	art3.sikes@s...	8/4/2016 1:1...	Never Retrie...	schoolz...	/Young Lady's School/staff/admin
bob bob	bob.bob@ys...	8/6/2016 1:0...	Never Retrie...	schoolz...	/test
Catherine Seely	Catherine.Se...	7/25/2016 9:...	Never Retrie...	schoolz...	/Young Stars School
Dean Cagle	Dean.Cagle...	8/5/2016 10:...	Never Retrie...	schoolz...	/Young Lady's School/staff/admin
Dennis Auger	Dennis.Auger...	7/15/2016 9:...	Never Retrie...	schoolz...	/Young Lady's School/students...
Edgar Bayles	Edgar.Bayles...	8/9/2016 12:...	Never Retrie...	schoolz...	/Young Stars School/students/...
Efrain2 Tague	Efrain2.Tagu...	8/2/2016 10:...	Never Retrie...	schoolz...	/Young Stars School/students/...
Emilio Freitag	emilio.freitag...	7/25/2016 9:...	Never Retrie...	schoolz...	/Young Lady's School/students...
Garry Heinrich	Garry.Heinric...	8/3/2016 8:2...	Never Retrie...	schoolz...	/Young Lady's School/staff/admin
Gerard Rhoa...	gerard.rhoad...	7/14/2016 11...	Never Retrie...	schoolz...	/Young Lady's School/staff
jiaping xu	jpxu@school...	8/9/2016 6:4...	Never Retrie...	schoolz...	/
Joey Albrecht	joey.albrecht...	8/2/2016 10:...	Never Retrie...	schoolz...	/Young Lady's School/staff
KeriNew Coc...	Keri.Cochran...	8/4/2016 1:1...	Never Retrie...	schoolz...	/Young Lady's School/test
Leann Bast	Leann.Bast@...	8/9/2016 12:...	Never Retrie...	schoolz...	/Young Stars School/students/...

The following options are available in the toolbar:

Clear Filter (filter icon)	Click the Clear Current Filter icon to clear the currently used filter.
Refresh	Click the Refresh icon to refresh the page.

The following columns of information are displayed for Google users:

Name	Chromebook user's name.
Email	Chromebook user's email address.
Last Login	Date and time when the user last logged into the domain.
Last Policy Retrieval	Date and time of the last endpoint profile retrieved by the Google Chromebook.
Domain	Name of the domain to which the user belongs.
Organizational Path	Organization path in the domain.

Viewing user details

You can view details about each user in a Google domain.

To view user details:

1. Go to *Google Domains* > *Domains*. The list of domains displays.
2. Click a domain. The list of Google users displays.
3. Click a Google user and scroll to the bottom of the content pane. The *User Details*, *Client Statistics*, and *Blocked Sites* panes display.

User Details

Field	Information
Name	User's name.
Email	User's email address.
Last Login	Date and time when the user last logged into the domain.
Last Policy Retrieval	Date and time of the last endpoint profile retrieved by the Google Chromebook.
Organization Path	Organization path of the user in the domain.
Effective Policy	Name of the profile assigned to the user in the domain.

Client Statistics

Charts	Information
Blocked Sites Distribution (past <number> days)	Displays the distribution of blocked sites in the past number of days. You can configure the number of days for which to display information. Go to *System Settings* > *Logs*.
Top 10 Site Categories by Distribution (Past <number> Days)	Displays the distribution of top ten site categories in the past number of days. You can configure the number of days for which to display information. Go to *System Settings* > *Logs*.

Blocked Sites (Past <number> Days)

Fields	Information
Time	Time the blocked site was visited.
Threat	Threat type detected.
Client Version	Chromebook user's current version.

Fields	Information
OS	Type of OS used by the Chromebook user.
URL	Blocked site's URL.
Port	Port number currently listening.
User Initiated	User initiated visitation to the blocked site.

Managing domains

You can manage domains from the *Google Domains* pane.

Editing domains

To edit domains:

1. Go to *Google Domains* > *Domains* and select a domain.
2. Click the *Edit* button.
3. Edit the options and click *Save Changes*.

Deleting domains

To delete domains:

1. Go to *Google Domains* > *Domains*, and select a domain.
2. Click the *Delete* button. A confirmation dialog displays.
3. Click *Yes*.

Quarantine Management

You can view and whitelist files quarantined by FortiSandbox or AntiVirus from a central management *Files* pane. You can also view and delete whitelisted files from the *Whitelist* pane.

Files

FortiClient sends quarantined file information to FortiClient EMS. The FortiClient EMS administrator can view quarantined file information for all managed endpoints on the *Files* pane and whitelist files from FortiClient EMS if needed.

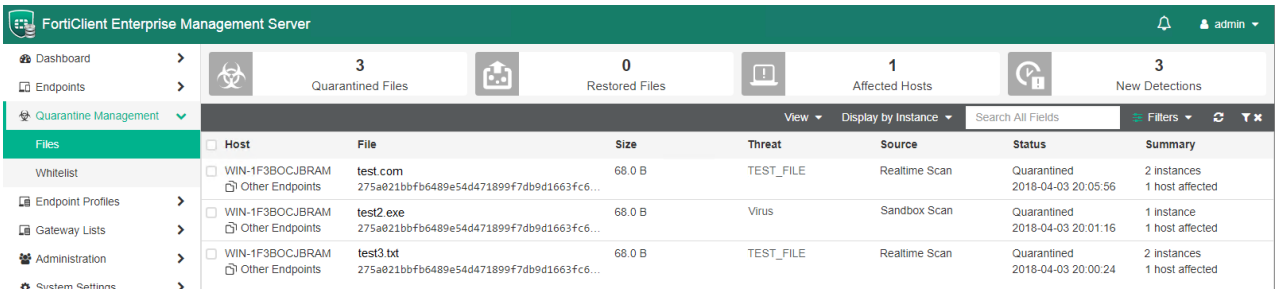
Viewing quarantined files

After FortiClient quarantines files on endpoints and sends the quarantined file information to FortiClient EMS, you can view the list of quarantined files in the Files pane. You can also view details about each quarantined file and use filters to access quarantined files with specific qualities.

Viewing the Files content pane

You can view information about quarantined files on the Files content pane.

1. Go to *Quarantine Management* > *Files*. The list of quarantined files, a quick status bar, and a toolbar display in the content pane.



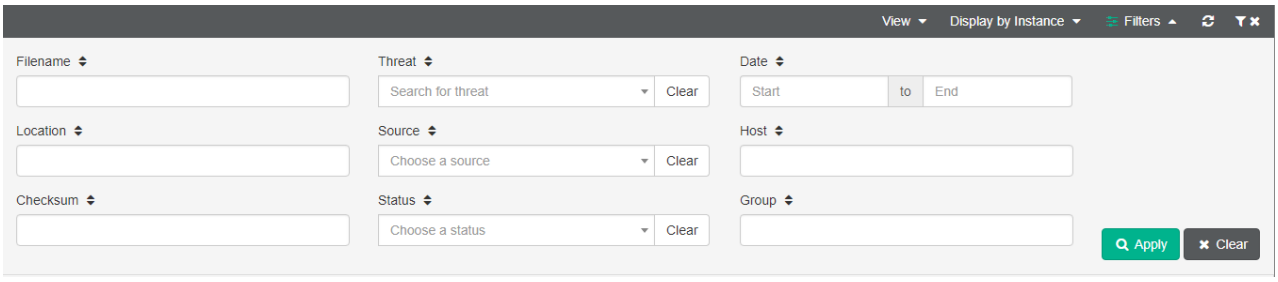
Quarantined Files	Number of files that have been quarantined on endpoints. Click to display the list of quarantined files.
Restored Files	Number of files that have been restored on endpoints. Click to display the list of restored files.
Affected Hosts	Number of hosts that have been affected by quarantined files. Click to display the list of quarantined files sorted by host name.
New Detections	Number of new detections. Click to display the list of newly detected threats sorted by date detected.

View	Select to toggle between the following options: • View all files or view only quarantined files • Show or hide full path names for files
Display by	Select to display the list of files by instance, host, threat, or date.
Search All Fields	Type a value and press *Enter* to search for the value in the list of files.
Filters	Click to display and hide filters you can use to filter the list of files.
Refresh	Click to refresh the list of files in the content pane.
Clear Filters	Click to clear all filters applied to the list of files.
Checkbox	Click to select all files displayed in the content pane.
Host	Hostname of the endpoint. Also shows the group the endpoint belongs to.
File	Name of the file.
Size	Size of the file in bytes.
Threat	Name of threat.
Source	Displays how the threat was detected: • Scheduled Scan • Email Scan • Startup Scan • Manual Scan • Realtime Scan • Rootkit Manual Scan • Sandbox Scan
Status	Status of the file: *Quarantined*, *Quarantined & Whitelisted*, *Restored*, or *Deleted*. Also shows the time the file was quarantined.
Summary	Displays the number of threat instances and number of affected hosts.

Filtering files list

You can filter the list of files displayed on the *Files* content pane.

1. Go to *Quarantine Management* > *Files*. The list of files displays.
2. Click the *Filters* menu, and set filters.
   The filter options display.
   For text values, you can use a comma (,) to separate values and an exclamation mark (!) to exclude a value.



Filename	Type the file name(s) to include in the filter. You can exclude a name or names from the filter using an exclamation mark (!).
Location	Type the file location(s) to include in the filter. You can exclude a location or locations from the filter using an exclamation mark (!).
Checksum	Type the checksum(s) to include in the filter. You can exclude a checksum or checksums from the filter using an exclamation mark (!).
Threat	Type the threat(s) to include in the filter. You can exclude a threat or threats from the filter using an exclamation mark (!). You can also select the desired threat(s) from the dropdown list.
Source	Type the source(s) to include in the filter. You can exclude a source or sources from the filter using an exclamation mark (!). You can also select the desired source(s) from the dropdown list.
Status	Type the status(es) to include in the filter. You can exclude a status or statuses from the filter using an exclamation mark (!). You can also select the desired statuse(s) from the dropdown list.
Date	Enter the range of dates to include in the filter.
Host	Type the host(s) to include in the filter. You can exclude a host or hosts from the filter using an exclamation mark (!). You can also select the desired host (s) from the dropdown list.
Group	Type the endpoint group(s) to include in the filter. You can exclude a group or groups from the filter using an exclamation mark (!). You can also select the desired group(s) from the dropdown list.

3. Click *Apply*.
   The filtered list of files displays.
4. Click *Clear Filters* to clear the filter settings.

Whitelisting quarantined files

You can whitelist and restored quarantined files. This releases the files from quarantine and makes them accessible on the endpoint with the next Telemetry communication between FortiClient EMS and FortiClient.

1. Go to *Quarantine Management* > *Files*.
2. Select the desired files.

3. Click *Whitelist & Restore*.
4. In the confirmation dialog, click *Yes*, then *Okay*. The file status changes to *Quarantined & Whitelisted*.

Whitelist

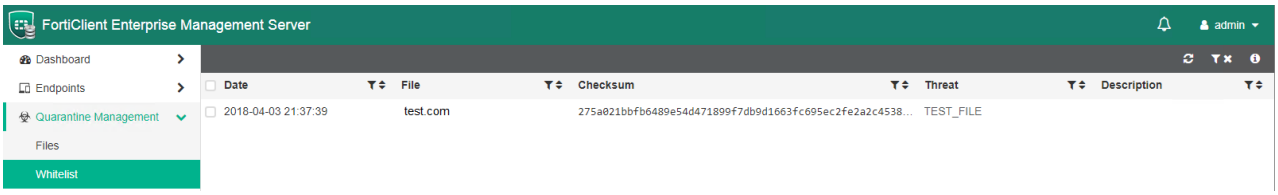
Viewing whitelisted files

You can view the list of whitelisted files in the Whitelist pane. You can also view details about each whitelisted file and use filters to access whitelisted files with specific qualities.

Viewing the Whitelist content pane

You can view information about whitelisted files on the Whitelist content pane.

1. Go to *Quarantine Management* > *Whitelist*. The list of whitelisted files and a toolbar display in the content pane.



Refresh	Click to refresh the list of files in the content pane.
Clear Filters	Click to clear all filters applied to the list of files.
Advanced Information	Click to view the FortiSandbox signature version and AV engine version.
Date	Date and time the file was whitelisted.
File	Name of the file.
Checksum	The file's checksum.
Threat	Name of threat.
Description	The file's description. Blank by default.

Filtering whitelisted files

You can filter the list of files displayed on the *Files* content pane.

1. Go to *Quarantine Management* > *Whitelist*. The list of files displays.
2. You can apply filters by date, file name, checksum, threat, and description. Do the following:
   a. To filter files by date, click the filter icon beside the *Date* heading. Select the desired date range in the *Start* and *End* fields. You can also enter a start time and end time on the selected dates. The default time is 12:00 PM.

b. To filter by file name, checksum, threat, or description, click the filter icon beside the desired heading. Type the value to include in the filter. You can toggle the *All/Any/Not* button for the following options:
   - *All:* Display all files that match the set filter.
   - *Any:* Display any file that matches the set filter.
   - *Not:* Display only files that do not match the set filter.

   The filtered list of files displays.

3. To remove a filter, click the *X* icon beside the filter. To remove all filters, click the *Clear Filters* icon on the toolbar.

Editing file descriptions

You can edit a whitelisted file's description. By default, the file description is blank.

1. Go to *Quarantine Management* > *Whitelist*.
2. Select the desired file.
3. Click *Edit Description*.
4. In the *Required* field, enter the desired description.
5. Click *Confirm*. The description appears under the *Description* heading.

Deleting files from the whitelist

You can delete files from the whitelist. This reverts the file's status to quarantined on the endpoint with the next Telemetry communication.

1. Go to *Quarantine Management* > *Whitelist*.
2. Select the desired file.
3. Click *Delete*.
4. In the confirmation dialog, click *Yes*. The file is deleted from the whitelist and will be quarantined on the endpoint with the next Telemetry communication. You can view the file on the *Files* pane.

Software Inventory

You can centrally view a list of software installed on all endpoints. The list includes details for each application such as vendor and version information. You can view this information by application or vendor on the *Applications* pane or by host on the *Hosts* pane. FortiClient sends installed application information to FortiClient EMS

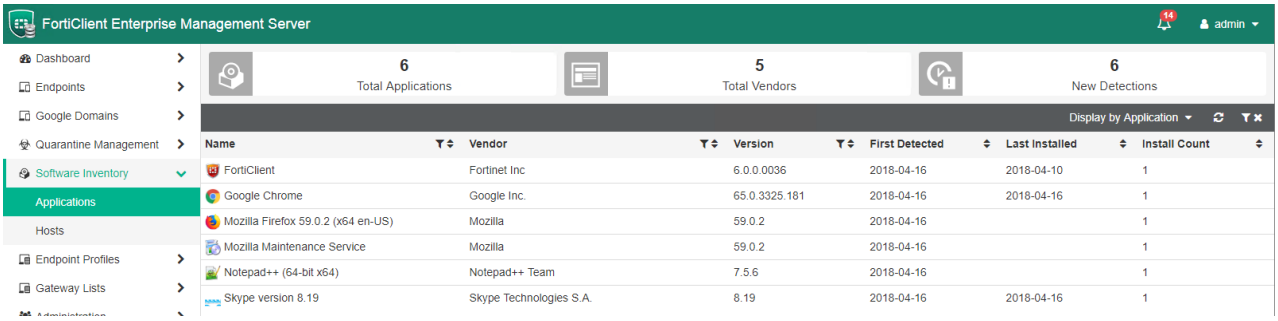
Applications

The FortiClient EMS administrator can view installed application information for all managed endpoints on the *Applications* pane.

Viewing the Applications content pane

You can view information about installed applications on the *Applications* content pane.

1. Go to *Software Inventory* > *Applications*. The list of applications, a quick status bar, and a toolbar display in the content pane.



Total Applications	Number of applications that have been installed on all managed endpoints. Click to display the list of installed applications.
Total Vendors	Number of vendors whose applications have been installed on managed endpoints. Click to display the list of installed applications sorted by vendor.
New Detections	Number of applications that have been detected as newly installed since the last Telemetry communication. Click to display newly detected applications sorted by date detected.
Display by	Select to toggle between the following options: • Display applications alphabetically by application name. • Sort applications by vendor name.
Refresh	Click to refresh the list of applications in the content pane.
Clear Filters	Click to clear all filters applied to the list of files.

Name	Name of the installed application.
Vendor	Name of the installed application's vendor.
Version	Version number of the installed application.
First Detected	Date the application was first detected as installed on the endpoint.
Last Installed	Date the application was last installed on an endpoint.
Install Count	Number of endpoints the application is installed on.

Filtering applications

You can filter the list of applications displayed on the *Applications* content pane.

1. Go to *Software Inventory* > *Applications*. The list of applications displays.
2. You can apply filters by application name, vendor name, and version number. Click the filter icon beside the desired heading. Type the value to include in the filter. You can toggle the *All/Any/Not* button for the following options:
   - *All:* Display all files that match the set filter.
   - *Any:* Display any file that matches the set filter.
   - *Not:* Display only files that do not match the set filter.
3. To remove a filter, click the *X* icon beside the filter. To remove all filters, click the *Clear Filters* icon on the toolbar.

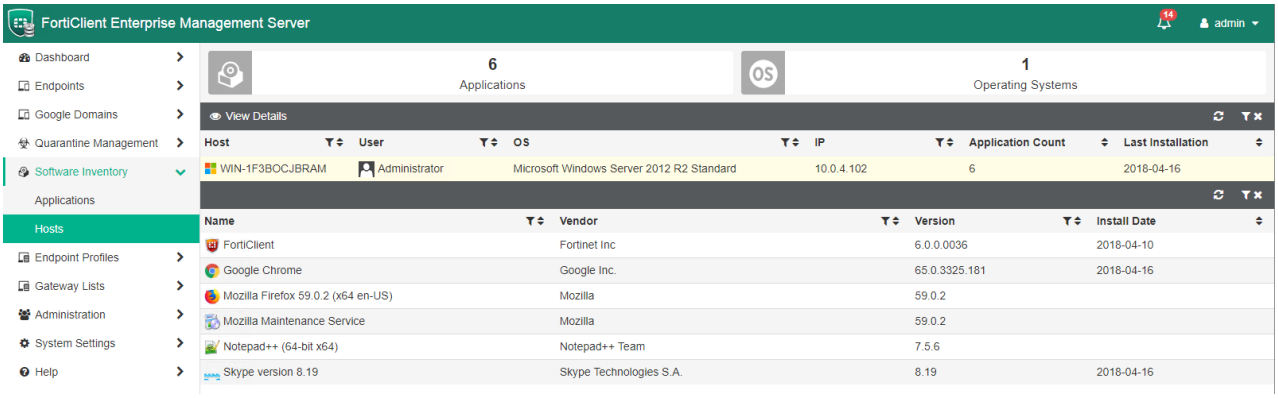
Hosts

The FortiClient EMS administrator can view installed application information for all managed endpoints by host on the *Hosts* pane.

Viewing the Hosts content pane

You can view information about installed applications by host on the *Hosts* content pane.

1. Go to *Software Inventory* > *Hosts*. The list of hosts, a quick status bar, and a toolbar display in the content pane.



Applications	Number of applications that have been installed on all managed endpoints.
Operating Systems	Number of different operating systems on managed endpoints.
View Details	Displays list of software installed on the selected endpoint. For details on the application list headings, see Viewing the Applications content pane on page 101.
Refresh	Click to refresh the list of applications in the content pane.
Clear Filters	Click to clear all filters applied to the list of files.
Host	Host name.
User	Name of the endpoint user.
OS	Operating system installed on the endpoint.
IP	IP address of the endpoint.
Application Count	Number of applications installed on the endpoint.
Last Installation	Date of the most recent application installation on the endpoint.

Filtering hosts

You can filter the list of hosts displayed on the *Hosts* content pane.

1. Go to *Software Inventory* > *Hosts*. The list of hosts displays.
2. You can apply filters by host name, user name, OS name, and IP address. Click the filter icon beside the desired heading. Type the value to include in the filter. You can toggle the *All/Any/Not* button for the following options:
   - *All:* Display all files that match the set filter.
   - *Any:* Display any file that matches the set filter.
   - *Not:* Display only files that do not match the set filter.
3. To remove a filter, click the *X* icon beside the filter. To remove all filters, click the *Clear Filters* icon on the toolbar.

To filter the list of applications installed on an endpoint, select the endpoint and click *View Details*. See Filtering applications on page 102 for details on filtering the list of applications.

Endpoint Profiles

You can use the default endpoint profile or create endpoint profiles for many configurations and situations.

Configuring profiles

You can create and configure separate profiles for Windows/Mac/Linux endpoints and for Chromebook endpoints. You can also edit the default profiles.

When you install FortiClient EMS, a default profile is created. This profile is applied to any groups you create. The default profile is designed to provide effective levels of protection. There are separate default profiles for Windows/Mac/Linux endpoints and for Chromebook endpoints.

Editing the default profile

You can edit the default profile to add or remove settings. You can revert to default settings by clicking *Revert to Default*.

To edit the default profile:

1. Do one of the following:
   a. To edit the default profile for Chromebooks, go to *Endpoint Profiles* > *Local Chromebook Profiles*, and click the *Default - Chromebooks* profile.
   b. To edit the default profile for other endpoints, go to *Endpoint Profiles* > *Local Profiles*, and click the *Default* profile.
2. Configure the settings on the tabs. See Profile references on page 117.
3. Click *Save* to save the profile.

Configuring profiles for Windows, Mac, and Linux endpoints

The default profile is designed to provide effective levels of protection. To use specific features, such as application firewall, create a new profile or change the default profile. Consider the following when creating profiles:

- Use default settings within a profile.
- Consider the endpoint's role when changing the default profile or creating new profiles.
- Create a separate group and profile for endpoints requiring long-term special configuration.
- Use FortiClient EMS for all central profile settings, and set options for within the group instead of for the endpoint itself when possible.

These topics describe creating and configuring profiles for Windows, Mac, and Linux endpoints.

Creating profiles to configure FortiClient

This section describes how to create a profile that excludes any installation or uninstallation of FortiClient software on endpoints. This type of profile is used to configure FortiClient software on endpoints.

To create profiles:

1. Go to *Endpoint Profiles* > *Manage Profiles*, and click the *Add* button. To create a Chromebook profile, click *Add Chrome*.
2. In the *Profile Name* box, type the profile name.
3. On the *Deployment* tab, leave *FortiClient Deployment* disabled.
4. Configure the settings on the remaining tabs. See Profile references on page 117.
5. Click *Save* to save the profile.

Creating profiles to deploy FortiClient

You must create a new profile to deploy FortiClient to endpoints. You cannot add a FortiClient installer to the default profile.

You must add FortiClient installers to FortiClient EMS before you can select the installers in a profile. See Adding FortiClient installers on page 141.

The selected FortiClient installer in a profile controls what tabs are displayed for configuration in the profile. Only the tabs for the features in the selected installer are displayed for configuration in the profile. For example, if the installer includes only the VPN feature, only the *VPN* tab is displayed for you to configure. The *System Settings* tab always displays.

You can disable a feature included in the installer, then enable the feature in the profile later. For example, if the installer includes the Web Filter and VPN features, you can disable the Web Filter feature and keep the VPN feature enabled. When FortiClient is installed on the endpoint, the Web Filter is installed, but disabled.

To create profiles for FortiClient deployment:

1. Go to *Endpoint Profiles* > *Manage Profile*, and click the *Add* button.
2. On the *Deployment* tab, enable *FortiClient Deployment*. The FortiClient deployment options display.
3. Set the following options on the *Deployment* tab:

Action		
	Assign an	Click *Installer*.
	Installer	In the *Installer* list, select a FortiClient installer. If you have not added a FortiClient installer to FortiClient EMS, see Adding FortiClient installers on page 141. The selected FortiClient installer affects what tabs display for configuration. Only tabs related to features enabled in the FortiClient installer display for configuration.
Schedule		
	Start At	Specify what time to start installing FortiClient on endpoints.

	Reboot When Needed	Enable to reboot the endpoint to install FortiClient when needed.
	Reboot when no users is logged in	Enable to allow the endpoint to reboot without prompt if no endpoint user is logged into FortiClient.
	Notify users and let the user decide when to reboot when they are logged in	Enable to notify the end user if a reboot of the endpoint is needed and allow the user to decide what time to reboot the endpoint. Disable to reboot the endpoint without notifying the user.
Credentials		
	Username	Type the username to perform deployment on AD. You must enter the admin credentials for the AD in the profile. Enter the appropriate credentials in the profile to assign to the AD. The credentials allow EMS to install FortiClient on endpoints using AD. If the credentials are wrong, the installation fails, and an error displays in EMS.
	Password	Type the password to perform deployment on AD.

4. Set the options on the remaining tabs.
5. Click *Save*.

Creating profiles to uninstall FortiClient

You can configure a profile to uninstall FortiClient from endpoints. You must create a new profile for this configuration. You cannot use the default profile to uninstall FortiClient from endpoints.

To create profiles to uninstall FortiClient:

1. Go to *Endpoint Profiles* > *Manage Profiles*, and click the *Add* button.
2. On the *Deployment* tab, enable *FortiClient Deployment*. The FortiClient deployment options display.

3. Set the following options on the *Deployment* tab:

Action		
	Assign an	Click *Uninstaller*.
Schedule		
	Start At	Specify what time to start uninstalling FortiClient from endpoints.
	Reboot When Needed	Enable to reboot the endpoint to install FortiClient when needed.
	Reboot when no users is logged in	Enable to allow the endpoint to reboot without prompt if no endpoint user is logged into FortiClient.
	Notify users and let the user decide when to reboot when they are logged in	Enable to notify the end user if a reboot of the endpoint is needed and allow the user to decide what time to reboot the endpoint. Disable to reboot the endpoint without notifying the user.
Credentials		
	Username	Type the username to perform deployment on AD or workgroups. If you are using an AD to uninstall FortiClient on endpoints, you must enter the admin credentials for the AD in the profile. If you are using a workgroup to uninstall FortiClient on endpoints, FortiClient must be connected to FortiClient EMS. Admin credentials are not required. When configuring the profile, know what method (AD or workgoup) is being used to uninstall FortiClient on endpoints. If using an AD, enter the appropriate credentials in the profile you will assign to the AD. The credentials allow EMS to uninstall FortiClient on endpoints by using AD. If the credentials are wrong, the uninstallation fails, and an error displays in EMS.
	Password	Type the password to perform the uninstall on AD or workgroups.

4. Click *Save*.

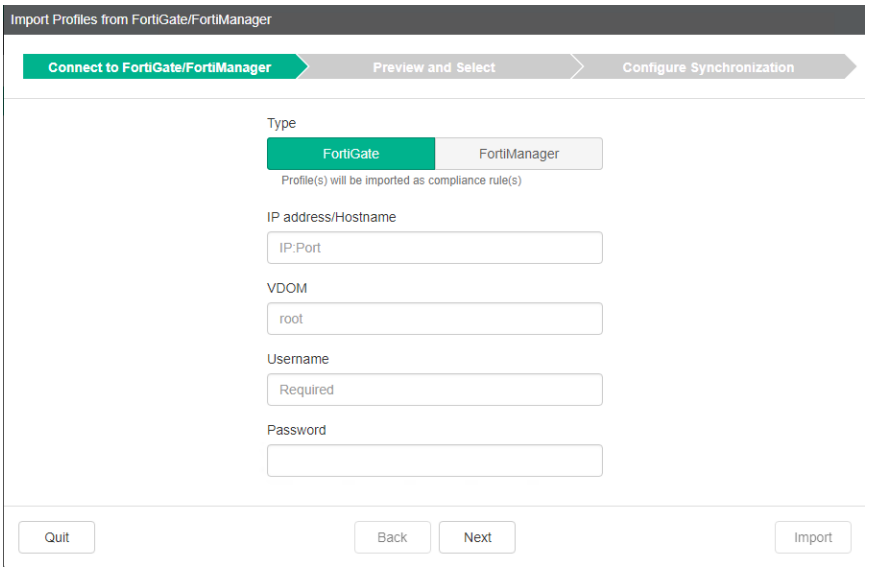
Importing FortiGate profiles

In FortiOS, endpoint profiles are called FortiClient Compliance profiles. You can import a FortiClient Compliance profile into EMS, then edit the profile in FortiClient EMS to add a FortiClient installer or add configuration information that supports the FortiGate compliance rules.

To import profiles successfully from FortiOS to FortiClient EMS, FortiGate must have the HTTPS port open. In FortiOS, go to *Network* > *Interfaces* > *Administrative Access* and enable the *HTTPS* checkbox.

To import profiles:

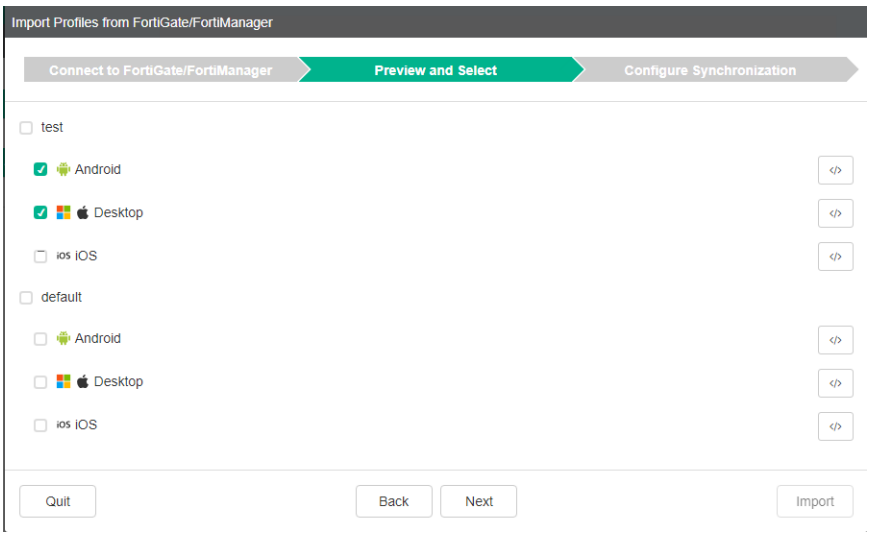
1. Click *Endpoint Profiles* > *Manage Profiles* > *Import*. The *Import Profiles from FortiGate/FortiManager* window opens.



2. Under *Type*, select *FortiGate*.
3. Complete the following options, and click *Next*.

IP address/Hostname	Enter the IP address and port of the FortiGate device from which the profile is being imported, in the format: `<ip address>:<port>`.
VDOM	Enter a VDOM name from the FortiGate if applicable.
Username	Enter the FortiGate's login username.
Password	Enter the FortiGate's login password.

The list of FortiClient Compliance profiles configured on the FortiGate displays.

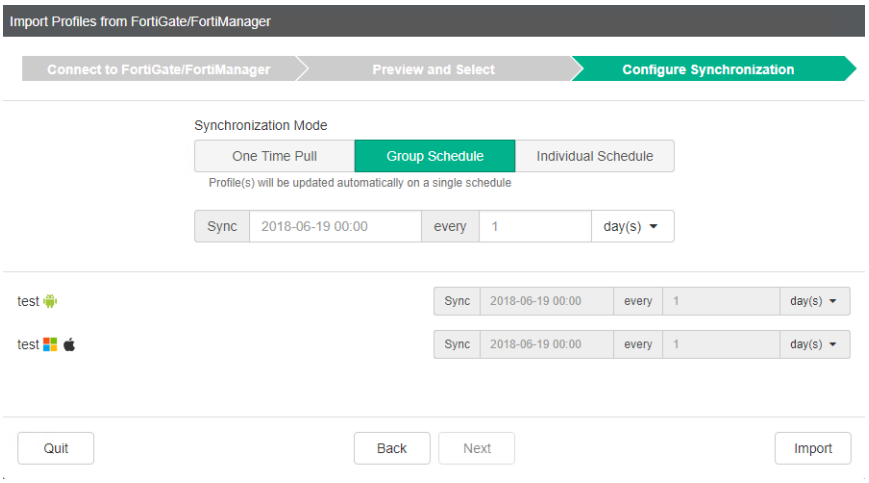


Under each profile name is the list of profiles created for different operating systems, such as desktops running a Windows or Mac operating system or devices running an Android operating system. In the example, under the test profile, *Android*, *Desktop*, and *iOS* profiles are listed. You can click the </> icon beside each profile to preview the settings in XML format.

4. Select the profiles to import into EMS and click *Next*.

   Select the name of the profile to import all profiles for it into EMS. You can also clear the checkbox beside the profiles you do not want to import into EMS. For example, you can import the Android and desktop profiles, but not the iOS profile for a given profile name.

5. Under *Synchronization Mode*, select one of the following options.



   a. *One Time Pull*: If selected, FortiClient EMS does not automatically sync profile changes from the FortiGate. You can manually sync profile changes after importing the profile. See Syncing profile changes on page 116.
   b. *Group Schedule*: Select to configure a group synchronization schedule for all selected profiles. Select the next date and time to automatically update the profiles, and the profile update interval in days, hours, or seconds.
   c. *Individual Schedule*: Select to configure an individual synchronization schedule for each selected profile. Select the next date and time to automatically update each profile, and the profile update interval in days, hours, or seconds.

6. Click *Import*. The selected profiles are imported into EMS and display under the *Endpoint Profiles* pane in a group named after the FortiGate device from which they were imported.
7. In the *Endpoint Profiles* page, select an imported profile to edit it.

   The options configured in the profile by the FortiGate administrator are read-only compliance rules. You cannot change them. You can edit additional options to provide configuration information to support the compliance rules. You can also add a FortiClient installer to the profile by using the *Deployment* tab. Custom installers can be created. See Adding FortiClient installers on page 141.
8. Edit the options on the tabs.
9. Click *Save Profile*.

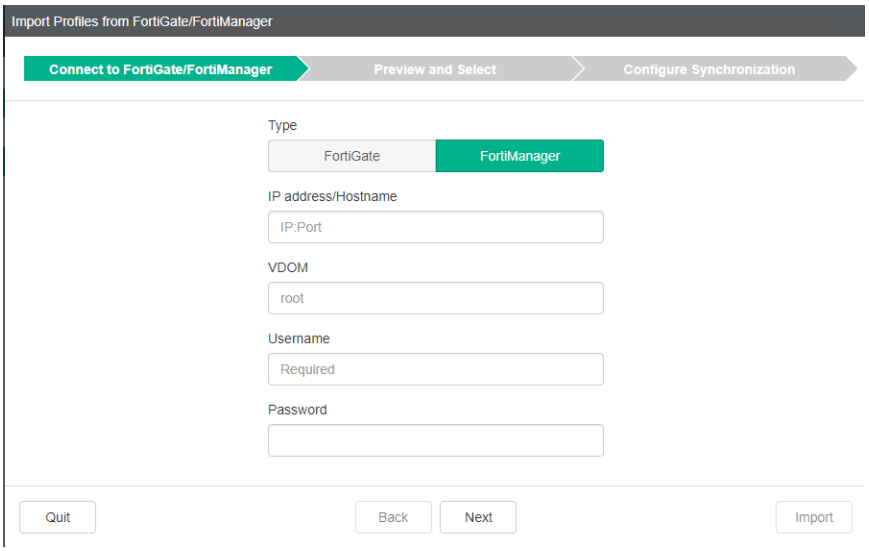
Importing FortiClient profiles from FortiManager

You can import FortiClient profiles from FortiManager into EMS, then edit the profile in FortiClient EMS to add a FortiClient installer or add configuration information that supports the FortiGate compliance rules.

To import profiles successfully from FortiManager to FortiClient EMS, FortiManager must have the HTTPS port open. In FortiManager, go to *System Settings* > *Network* and enable the *HTTPS* checkbox.

To import profiles:

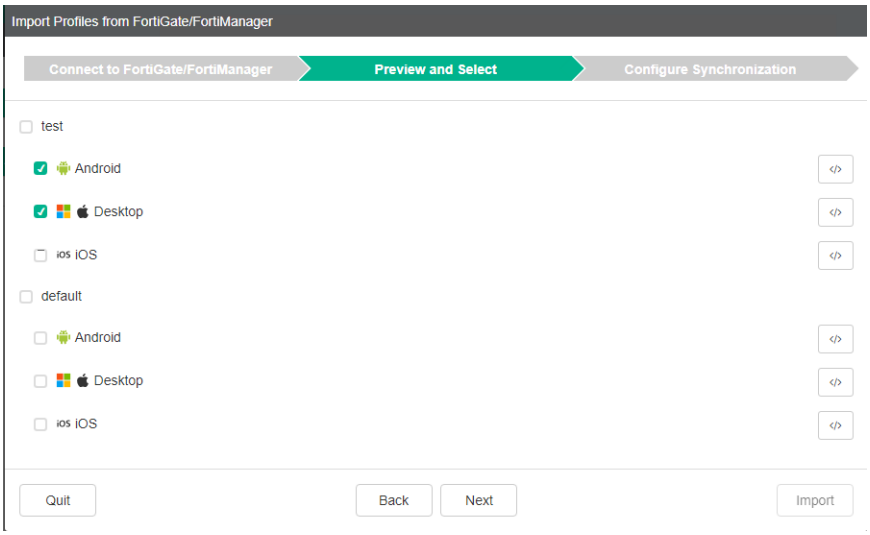
1. Click *Endpoint Profiles* > *Manage Profiles* > *Import*. The *Import Profiles from FortiGate/FortiManager* window opens.



2. Under *Type*, select *FortiManager*.
3. Complete the following options, and click *Next*.

IP address/Hostname	Enter the IP address and port of the FortiManager device from which the profile is being imported, in the format: `<ip address>:<port>`.
VDOM	Enter a VDOM name from the FortiManager if applicable.
Username	Enter the FortiManager's login username.
Password	Enter the FortiManager's login password.

The list of FortiClient profiles configured on the FortiManager displays.

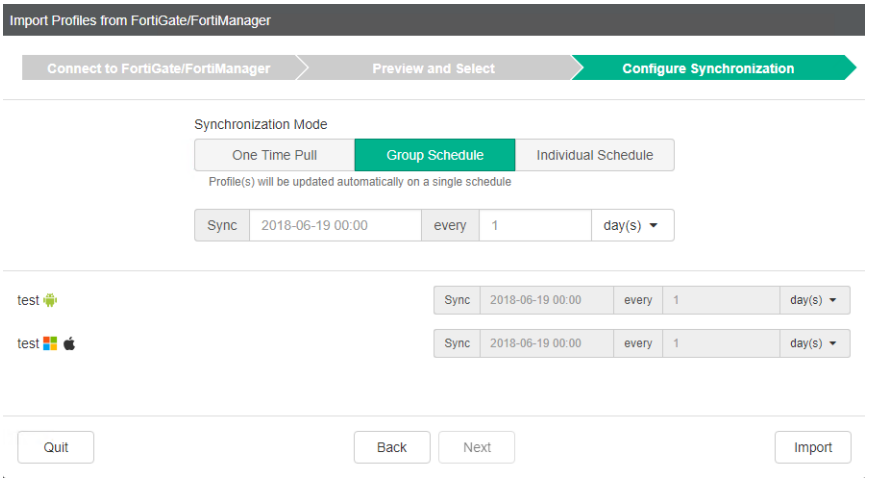


Under each profile name is the list of profiles created for different operating systems, such as desktops running a Windows or Mac operating system or devices running an Android operating system. In the example, under the test profile, *Android*, *Desktop*, and *iOS* profiles are listed. You can click the </> icon beside each profile to preview the settings in XML format.

4. Select the profiles to import into EMS and click *Next*.

   Select the name of the profile to import all profiles for it into EMS. You can also clear the checkbox beside the profiles you do not want to import into EMS. For example, you can import the Android and desktop profiles, but not the iOS profile for a given profile name.

5. Under *Synchronization Mode*, select one of the following options.



   a. *One Time Pull*: If selected, FortiClient EMS does not automatically sync profile changes from the FortiManager. You can manually sync profile changes after importing the profile. See Syncing profile changes on page 116.

   b. *Group Schedule*: Select to configure a group synchronization schedule for all selected profiles. Select the next date and time to automatically update the profiles, and the profile update interval in days, hours, or seconds.

   c. *Individual Schedule*: Select to configure an individual synchronization schedule for each selected profile. Select the next date and time to automatically update each profile, and the profile update interval in days, hours, or seconds.

6. Click *Import*. The selected profiles are imported into EMS and display under the *Endpoint Profiles* pane in a group named after the FortiManager device from which they were imported.
7. In the *Endpoint Profiles* page, select an imported profile to edit it.

   You can edit additional options to provide configuration information to support the compliance rules. You can also add a FortiClient installer to the profile by using the *Deployment* tab. Custom installers can be created. See Adding FortiClient installers on page 141.
8. Edit the options on the tabs.
9. Click *Save Profile*.

Creating profiles with XML

You can configure FortiClient profile settings in FortiClient EMS by using XML or a custom XML configuration file. The custom XML file must include all settings required by the endpoint at the time of deployment. For more information about how to configure a profile with XML, see the *FortiClient XML Reference* on docs.fortinet.com.

To create profiles with XML:

1. Go to *Endpoint Profiles* > *Manage Profiles*, and click the *Add* button.
2. In the *Profile Name* box, type a name for the profile.
3. Click the *Advanced* button. The *XML Configuration* tab displays, and the profile configuration displays in XML.
4. Click the *XML Configuration* tab, and click the *Edit* button.
5. Edit the XML.
6. Click *Test XML*.
7. Click *Save* to save the profile.

Creating profiles to automatically upgrade FortiClient

You can create a profile to automatically upgrade FortiClient to the latest patch release. The profile must be configured with an installer that meets the following requirements:

- The FortiClient installer was created in FortiClient EMS 1.2.0 or later.
- The FortiClient installer was created with the latest FortiClient version available for selection in FortiClient EMS at the time the installer was created.
- The FortiClient installer was created with the *Keep software updated to the latest patch release* option enabled.

See Adding FortiClient installers on page 141 for details on creating an installer.

With this configuration, when an upgrade is available, FortiClient downloads it directly from the FortiClient EMS server. Offline FortiClients remain without the upgrade until they contact the FortiClient EMS server.

To create profiles to automatically upgrade FortiClient:

1. Go to *Endpoint Profiles* > *Manage Profiles*, and click the *Add* button.
2. In the *Profile Name* box, type a name for the profile.
3. On the *Deployment* tab, enable *FortiClient Deployment*.
4. Beside *Assign an*, click *Installer*.
5. From the *Installer* dropdown list, select the desired installer, or use the *Create a New Installer* button.
6. Configure the profile as desired, then click *Save Profile*.

If deploying an upgrade to a FortiClient endpoint running Windows 7, the *Enable TLS 1.0/1.1* option must be enabled. See Configuring Server settings on page 167.

Configuring profiles for Chromebooks

Chromebook profiles support web filtering by categories, black and white lists, and safe search. You can create different profiles and assign them to different groups in the Google domain.

These topics describe creating and configuring profiles for Chromebook endpoints.

Adding new profiles

When you install FortiClient EMS, a default profile is created. This profile is applied to any domains you add to FortiClient EMS.

It is recommended to add Yandex search engine to the black list in the profile.

To create new profiles:

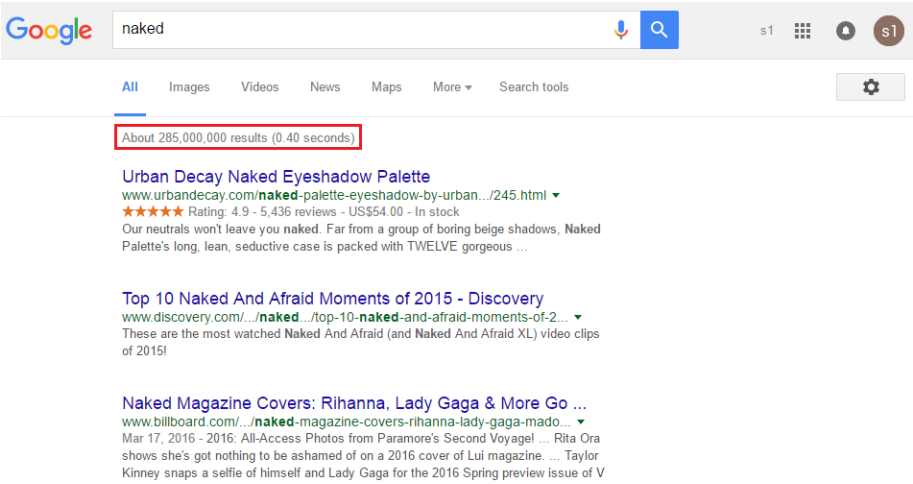
1. Go to *Endpoint Profiles* > *Manage Profiles*, and click the *Add Chrome* button.
2. In the *Profile Name* box, type the profile name.
3. On the *Web Filter* tab, enable *Web Filter*, and set the web filtering options.
4. On the *System Settings* tab, set the logging options.
5. Click *Save*.

Enabling/disabling safe search

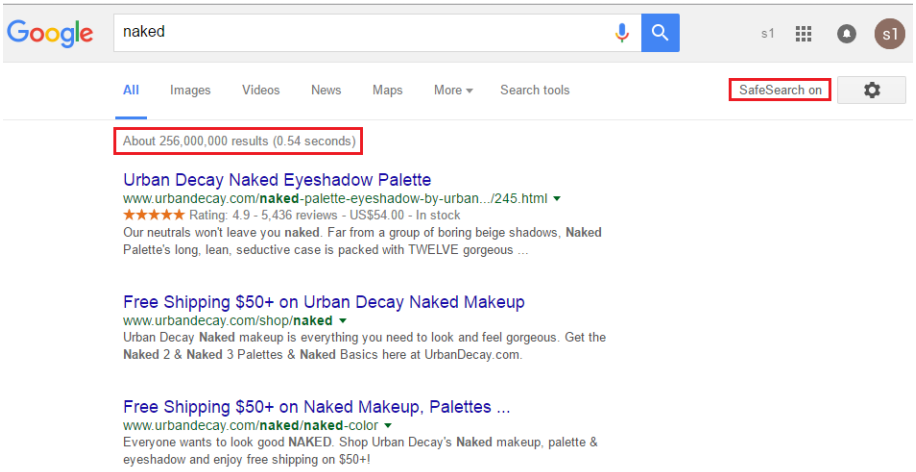
The search engine provides a Safe Search feature that blocks inappropriate or explicit images from search results. The Safe Search feature helps avoid most adult content. FortiClient EMS supports Safe Search for most common search engines, such as Google, Yahoo, and Bing.

The profile in FortiClient EMS controls the Safe Search feature.

Following are examples of search results with the Safe Search feature disabled and enabled. Notice the difference between the number of results. Here are the search results when the Safe Search feature is disabled, which has about 285000000 results:



Here are the search results when the Safe Search feature is enabled, which has about 256000000 results.



To enable or disable Safe Search:

1. In FortiClient EMS, in the *Endpoint Profiles* > *Manage Profiles* area, click the *Default - Chromebooks* profile or another profile.
2. On the *Web Filter* tab, enable or disable *Enable Safe Search*.

Viewing profiles

When you create endpoint profiles, they are listed under *Endpoint Profiles* in the left pane. You can view endpoint profiles and their settings.

To view profiles:

1. Go to *Endpoint Profiles* > *Manage Profiles*. The content pane displays the list of profiles.
2. Click a profile name, then click *Edit*. The settings display in the content pane.

Assigning profiles

- Assigning profiles to Windows, Mac, and Linux endpoints on page 115
- Assigning profiles to Chromebooks on page 115

Assigning profiles to Windows, Mac, and Linux endpoints

After creating the profile, you can assign the profile to domains or workgroups. When you assign the profile to domains or workgroups, the profile settings are automatically pushed to the endpoints in the domain or workgroup.

If you do not assign a profile to a specific domain or workgroup, the default profile is automatically applied.

To assign profiles:

1. Go to *Endpoints*.
2. Right-click a domain or group, select *Assign profile*, then the profile. A confirmation dialog box displays.
3. Click *Yes*. The profile is assigned.

Assigning profiles to Chromebooks

After creating the profile, you can assign the profile to Google domains. When you assign the profile to domains, the profile settings are automatically pushed to the Chromebooks in the domain.

To assign profiles:

1. Go to *Google Domains*.
2. Right-click a domain, select *Assign Profile*, then the profile. The profile is assigned.
3. Hover the mouse over the name of the domain to view the name of the assigned profile.

Managing profiles

You can manage profiles from the *Endpoint Profiles* pane.

Editing profiles

When you edit a profile assigned to endpoints or domains, the changes are automatically pushed to the endpoints or Chromebooks when you save the profile.

To edit profiles:

1. Go to *Endpoint Profiles*, and select a profile.
2. Click *Edit*. The profile settings display in the content pane.

3. Edit the settings. See Profile references on page 117.
4. Click *Save*. If the profile is assigned to endpoints/domains, the changes are pushed to the endpoints/domains.

Cloning profiles

To clone profiles:

1. Go to *Endpoint Profiles* > *Manage Profiles*.
2. Select a profile, and click the *Clone* button. The cloned profile displays in the content pane.
3. In the *Profile Name* box, type a name for the profile.
4. Configure the settings on the tabs. See Profile references on page 117.
5. Click *Save*.

Syncing profile changes

For profiles imported from FortiGate or FortiManager, you can manually sync profiles so they are updated with the latest changes from the FortiGate or FortiManager they were imported from.

1. Go to *Endpoint Profiles* > *Manage Profiles*.
2. Select the desired profile.
3. Click *Sync Now*.

Editing sync schedules

For profiles imported from FortiGate or FortiManager, you can edit the sync schedule.

1. Go to *Endpoint Profiles* > *Manage Profiles*.
2. Select the desired profile.
3. Click *Edit Sync Schedule*.
4. In the *Synchronization Settings* window, configure the following options:
   a. *One Time Pull*: If selected, FortiClient EMS does not automatically sync profile changes from the FortiGate. You can manually sync profile changes after importing the profile. See Syncing profile changes on page 116.
   b. *Group Schedule*: Select to configure a group synchronization schedule for all selected profiles. Select the next date and time to automatically update the profiles, and the profile update interval in days, hours, or seconds.
   c. *Individual Schedule*: Select to configure an individual synchronization schedule for each selected profile. Select the next date and time to automatically update each profile, and the profile update interval in days, hours, or seconds.

Deleting profiles

You cannot delete the default profiles.

To delete profiles:

1. Go to *Endpoint Profiles* > *Manage Profiles*.
2. Click desired profile, then click the *Delete* button. A popup displays.
3. Click *Yes*. The profile is deleted.

Profile references

This section contains descriptions of the tabs and options used to configure profiles.

Note that for Chromebooks, only the *Web Filter* and *System Settings* tabs are available. All other tabs are exclusive to Windows, macOS, and Linux endpoints.

Profile Name

Option	Description
Profile Name	Type a name for the profile.
Basic	Select to display the basic options for configuration.
Advanced	Select to configure the profile using XML on the *XML Configuration* tab. Displays advanced options for configuration. This option is only available for Windows, Mac, and Linux profiles.

AntiVirus Protection

Enable antivirus protection. Some options only display if you enable *Advanced* view. Configure the following options:

Options	Description
AntiVirus Protection	Toggle to enable or disable AntiVirus protection.
Real-Time Protection	
Action On Virus Discovery	• Warn the User If a Process Attempts to Access Infected Files • Quarantine Infected Files. You can use FortiClient to view, restore, or delete the quarantined file, as well as view the virus name, submit the file to FortiGuard, and view logs. • Deny Access to Infected Files • Ignore Infected Files
Alert When Viruses Are Detected	If enabled, displays the *Virus Alert* dialog when a virus is detected while attempting to download a file via a web browser. The dialog allows you to view recently detected viruses, their locations, and statuses.

Options		Description
Identify Malware and Exploits Using Signatures Received from FortiSandbox		If enabled, uses signatures from FortiSandbox to identify malware and exploits. This option is available only if the *Sandbox Detection* tab is enabled. Enter the number of minutes after which to update signatures.
Block Known Communication Channels Used by Attackers		Enable or disable C&C detection using IRDB signature. Check network traffic against known Command and Control Communication IP address plus port number combinations.
Block Access to Malicious Websites		Block all access to malicious websites. You must select *FortiProxy (Disable Only When Troubleshooting)* on the *System Settings* tab before you can enable this option.
	Security Risk	You can configure an action for all websites categorized as security risks. Select one of the following: • Block • Warn • Allow • Monitor Click the + button to view all security risk subcategories and configure individual actions (Block, Warn, Allow, Monitor) for each subcategory: • Dynamic DNS • Malicious Websites • Newly Observed Domain • Newly Registered Domain • Phishing • Spam URLs
	Use the Exclusion List Defined in the Web Filter Profile	If this option is enabled, the exclusion list on the *Web Filter* tab is used. If this option is not enabled, you must define exclusions under *Exclusions*.
Scan Compressed Files		Enable to scan archive files, including zip, rar, and tar files, for threats. Default file extensions are listed in RTP exclusions below.
	Max Size	Only scan files under the specified size. To allow scanning compressed files of any size, enter 0.
Scan Files Accessed by User Process		Configure when RTP should scan files accessed by the user process. Select one of the following: • Scan Files When Processes Read or Write Them • Scan Files When Processes Read Them • Scan Files When Processes Write Them
Scan Network Files		Enable to scan network files for threats when the user process accesses them.

Options	Description
System Process Scanning	Enable system process scanning. Select one of the following: • Scan Files When System Processes Read or Write Them • Scan Files When System Processes Read Them • Scan Files When System Processes Write Them • Do Not Scan Files When System Processes Read or Write Them
On Demand Scanning	
Action On Virus Discovery	Select one of the following from the dropdown list: • Warn the User If a Process Attempts to Access Infected Files • Quarantine Infected Files. You can use FortiClient to view, restore, or delete the quarantined file, as well as view the virus name, submit the file to FortiGuard, and view logs. • Ignore Infected Files
Integrate FortiClient into Windows Explorer's Context Menu	Adds a *Scan with FortiClient AntiVirus* option to the Windows Explorer right-click menu.
Pause Scanning When Running on Battery Power	Enable to pause scanning when the computer is running on battery power.
Automatically Submit Suspicious Files to FortiGuard for Analysis	Enable to automatically submit suspicious files to FortiGuard for analysis. You do not receive feedback for files submitted for analysis. The FortiGuard team is able to create signatures for any files that are submitted for analysis and determined to be malicious.
Scan Compressed Files	Enable to scan archive files, including zip, rar, and tar files, for threats.
Max Size	Only scan files under the specified size. To allow scanning compressed files of any size, enter 0.
Max Scan Speed on Computers With	Select the minimum amount of memory that must be installed on a computer to maximize scan speed. Antivirus will maximize scan speed by loading signatures on computers with a minimum amount of memory: • 4 GB • 6 GB • 8 GB • 12 GB • 16 GB
Scheduled Scan	Enable scheduled scans.
Schedule Type	Select *Daily*, *Weekly*, or *Monthly*.

Options		Description
Scan On		If *Weekly* is selected, select the day of the week to perform the scan. If *Monthly* is selected, select the day of the month to perform the scan. Note that if you configure monthly scans to occur on the 31st of each month, the scan occurs on the first day of the month for months with fewer than 31 days.
Start At		Configure the start time for the scheduled scan.
Scan Type		Select *Quick*, *Full*, or *Custom*.
	Quick	Runs the rootkit detection engine to detect and remove rootkits. The quick scan only scans the following items for threats: executable files, DLLs, and drivers that are currently running.
	Full	Runs the rootkit detection engine to detect and remove rootkits, then performs a full system scan of all files, executable files, DLLs, and drivers. If *Full* is selected, you have the following options: • Scan removable media, if present • Scan network drives
	Custom	Runs the rootkit detection engine to detect and remove rootkits. In the *Folder* field, enter the full path of the folder on your local hard disk drive that will be scanned.
Scan Priority		Set to *Low*, *Normal*, or *High*. This refers to the amount of processing power the scan uses and its impact on other processes.
Scan Removable Media		Enable to scan connected removable media, such as USB drives, for threats, if present.
Scan Network Drives		Enable to scan attached or mounted network drives for threats.
Enable Scheduled Scans Even When a Third-Party AV Product Is Present		Enable scheduled scans even when a third party AV product is present.
Anti-Exploit		Toggle to enable anti-exploit engine to monitor commonly used applications for attempts to exploit known vulnerabilities.
Show System Tray Notifications		Enable to show system tray notifications when an exploit is detected.
Application Exclusion List		Select applications to exclude from anti-exploit detection.

Options	Description
Exclusions	Enable exclusions from antivirus scanning. FortiClient EMS supports using wildcards and path variables to specify files and folders to exclude from scanning. The following wildcards and variables are supported, among others: • Using wildcards to exclude a range of file names with a specified extension, such as Edb*.jrs • Using wildcards to exclude all files with a specified extension, such as *.jrs • Path variable %windir% • Path variable %allusersprofile% • Path variable %systemroot% • Path variable %systemdrive% Note that having a longer exclusion list affects antivirus performance. It is advised to keep the exclusion list as short as possible.
Paths to Excluded Folders	Enter fully qualified excluded folder paths in the provided text box to exclude these folders from RTP and on-demand scanning.
Paths to Excluded Files	Enter fully qualified excluded files in the provided text box to exclude these files from RTP and on-demand scanning.
File Extensions Excluded from Real-Time Protection	Realtime AV protection skips scanning files with the specified extensions.
File Extensions Excluded from On Demand Scanning	On demand AV protection skips scanning files with the specified extensions.
Other	
Scan for Rootkits	Enable to scan for files implementing advanced OS hooks used by malware to protect themselves from being shutdown, killed, or deleted. A rootkit is a collection of programs that enable administrator-level access to a computer or computer network. Typically a rootkit is installed on a computer after first obtaining user-level access by exploiting a known vulnerability or cracking a password.
Scan for Adware	Enable to scan for adware. Adware is a form of software that downloads or displays unwanted ads when a user is online.
Scan for Riskware	Enable to scan for riskware. Riskware refers to legitimate programs which, when installed and executed, presents a possible but not definite risk to the computer.
Enable Advanced Heuristics	Enable AV scan with heuristics signature. Advanced heuristics is a sequence of heuristics to detect complex malware.

Options	Description
Scan Removable Media on Insertion	Enable to scan removable media (CDs, DVDs, Blu-ray disks, USB keys etc.) on insertion.
Scan Email	Enable to scan emails for threats with SMTP and POP3 protocols.
Scan MIME files (Inbox Files)	Enable to scan inbox email content with MIME file types. Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of the email to support the following: • Text in character sets other than ASCII • Non text attachments (audio, video, images, applications) • Message bodies with multiple parts
Enable FortiGuard Analytics	Automatically sends suspicious files to FortiGuard for analysis.
Notify Logged in Users if Their AV Signatures Expired	Enable to notify logged in users if their AntiVirus signatures have expired.

Sandbox Detection

Enable Sandbox Detection. Some options only display if you enable *Advanced* view. Configure the following options:

Options		Description
Sandbox Detection		Enable or disable Sandbox Detection.
Server		
	FortiSandbox	Select the desired FortiSandbox unit from the list of FortiSandbox units configured on the *Manage FortiSandboxes* pane. See Managing FortiSandbox units on page 146.
	Wait for FortiSandbox Results before Allowing File Access	Enable to have the endpoint user wait for FortiSandbox scanning results before being allowed access to files. Set the timeout in seconds. Disable to allow the endpoint user to access files before FortiSandbox results are provided.
	Deny Access to File When There Is No Sandbox Result	You have the option to: • Deny Access to Downloaded Files If FortiSandbox Is Offline. • Enter the *Timeout* value in seconds. File access is allowed if FortiSandbox results are not received when the timeout expires. Set to `-1` to infinitely restrict access to the file.
File Submission Options		

Options		Description
	All Files Executed from Removable Media	Select to submit all files executed on removable media, such as USB drives, to FortiSandbox for analysis.
	All Files Executed from Mapped Network Drives	Enable to submit all files executed from mapped network drives.
	All Web Downloads	Enable to submit all web downloads.
	All Email Downloads	Enable to submit all email downloads.
Remediation Actions		
	Action	Choose *Quarantine* or *Alert & Notify* for infected files.
Exceptions		
	Exclude Files from Trusted Sources	Enable to not submit files signed by trusted sources.
	Exclude Specified Folders/Files	Enable to exclude specified folders/files. You must also create the exclusion list.

Web Filter

For Windows, Mac, and Linux profiles, you must enable *FortiProxy (Disable Only When Troubleshooting)* on the *System Settings* tab to use the *Web Filter* options.

Configuration		Description
Web Filter		Enable or disable web filtering.
General		
	Client Web Filtering When On-Net	Enable client web filtering when on-net. Only available for Windows and Mac profiles. This setting affects the *Block Access to Malicious Websites* setting in AntiVirus Protection on page 117.
	Log All URLs	Enable to log all URLs.
	Log User Initiated Traffic	Enable to log user initiated traffic.
	Show Bubble Notification When HTTPS Site Is Blocked	Enable to show a bubble notification when an HTTPS site is blocked.

Configuration		Description
	Enable Safe Search	Enable safe search. Only available for Chromebook profiles. When safe search is enabled, the endpoint's Google search is set to *Restricted mode*, and YouTube access is set to *Strict Restricted access*. To set YouTube access to *Moderate Restricted* or *Unrestricted YouTube access*, you can disable Safe search and configure Google Search and YouTube access with the Google Admin Console instead of FortiClient EMS for Chromebooks.
Site Categories		Select to enable site categories from FortiGuard. When site categories are disabled, FortiClient is protected by the exclusion list. See the FortiGuard website for descriptions of the available categories and subcategories. For all categories below, you can configure an action for the entire site category by selecting one of the following: • Block • Warn • Allow • Monitor You can also click the + button beside the site category to view all subcategories and configure individual actions (Block, Warn, Allow, Monitor) for each subcategory. Each site category's subcategories are listed below.
	Adult/Mature Content	• Abortion • Advocacy Organizations • Alcohol • Alternative Beliefs • Dating • Gambling • Lingerie and Swimsuit • Marijuana • Nudity and Risque • Other Adult Materials • Pornography • Sex Education • Sports Hunting and War Games • Tobacco • Weapons (Sales)

Configuration		Description
	Bandwidth Consuming	• File Sharing and Storage • Freeware and Software Downloads • Internet Radio and TV • Internet Telephony • Peer-to-peer File Sharing • Streaming Media and Download
	General Interest-Business	• Armed Forces • Business • Charitable Organizations • Finance and Banking • General Organizations • Government and Legal Organizations • Information Technology • Information and Computer Security • Online Meeting • Remote Access • Search Engines and Portals • Secure Websites • Web Analytics • Web Hosting • Web-based Applications

Configuration		Description
	General Interest-Personal	• Advertising • Arts and Culture • Auction • Brokerage and Trading • Child Education • Content Servers • Digital Postcards • Domain Parking • Dynamic Content • Education • Entertainment • Folklore • Games • Global Religion • Health and Wellness • Instant Messaging • Job Search • Meaningless Content • Medicine • News and Media • Newsgroups and Message Boards • Personal Privacy • Personal Vehicles • Personal Websites and Blogs • Political Organizations • Real Estate • Reference • Restaurant and Dining • Shopping • Social Networking • Society and Lifestyles • Sports • Travel • Web Chat • Web-based Email

Configuration		Description
	Potentially Liable	• Child Abuse • Discrimination • Drug Abuse • Explicit Violence • Extremist Groups • Hacking • Illegal or Unethical • Plagiarism • Proxy Avoidance
	Unrated	
	Rate IP Addresses	Enable to filter URLs and resolved IP addresses at the same time.
Exclusion List		
Action		Select one of the following actions: • Allow • Block • Monitor
URL		Enter specific URLs to allow, block, or monitor.
Type		Select one of the following types: • Simple • Wildcard • Regular Expression Wildcard characters and Perl Compatible Regular Expressions (PCRE) can be used.

Application Firewall

Configuration	Description
Application Firewall	Enable or disable application control.
Notification Bubbles on User's Desktop When Applications Are Blocked	Enable notification bubbles when applications are blocked.
Detect & Block Exploits	Enable to inspect network traffic for intrusions attempting to exploit known vulnerabilities

Configuration	Description
Categories	Enable FortiClient firewall to allow, block or monitor applications based on their signature Block, allow or monitor the following categories: 1. Botnet 2. Business 3. Cloud.IT 4. Collaboration 5. Email 6. File.Sharing 7. Game 8. General.Interest 9. IM 10. Industrial 11. Mobile 12. Network.Service 13. P2P 14. Proxy 15. Remote.Access 16. Social.Media 17. Special 18. Storage.Backup 19. Update 20. Video/Audio 21. VoIP 22. Web.Others 23. All Other Unknown Applications
Application Overrides	Enable FortiClient firewall to allow, block or monitor applications based on their signature.
Delete	Delete an application.
Add Signature	Add a signature to an application.

VPN

Configuration	Description
VPN	Enable or disable VPN use.
General	

Configuration		Description
	Allow Personal VPN	Enable to allow users to create, modify and use personal VPN configurations.
	Disable Connect/Disconnect	Enable to disable connect/disconnect.
	Show VPN before Logon	Enable to allow users to select a VPN connection before logging into the system.
	Use Windows Credentials	Enable to connect using the current username and password.
	Minimize FortiClient Console On Connect	Enable to minimize the window upon connecting.
	Show Connection Progress	Display information on FortiClient dashboard while establishing connections.
	Use Vendor ID	Enable to use vendor ID. Enter the vendor ID in the Vendor ID box.
	Current Connection	Select the current VPN tunnel.
	Keep Running Max Tries	The maximum number of attempts to retry a VPN connection that was lost due to network issues. If set to 0, it will retry indefinitely
SSL VPN		Enable SSL VPN.
	DNS Cache Service Control	FortiClient disables Windows DNS cache when an SSL VPN tunnel is established. The DNS cache is restored after the SSL VPN tunnel is disconnected. If it is observed that FSSO clients do not function correctly when an SSL VPN tunnel is up, use the setting *Prefer SSL VPN DNS* to control the DNS cache.
	Prefer SSL VPN DNS	When disabled, custom DNS server from SSL VPN will not be added to physical interface. When enabled, custom DNS server from SSL VPN will be prepended to physical interface.
IPSec VPN		Enable IPSec VPN.

Configuration	Description
	Enable or disable the following: 1. Beep If Connection Fails 2. Use Windows Store Certificates a. Current User Windows Store Certificates (IPsec only) b. Local Computer Windows Store Certificates (IPSec only) 3. Use Smart Card Certificates 4. Show Auth Certificates Only 5. Block IPv6 6. Enable UDP Checksum 7. Disable Default Route 8. Check for Certificate Private Key 9. Enhanced Key Usage Mandatory

The following options are available in the *Creating VPN Tunnel* window after clicking the *Add Tunnel* button in the *VPN Tunnels* section.

Basic Settings		
	Name	Enter a VPN name.
	Type	Select *SSL VPN* or *IPsec VPN*.
	Remote Gateway	Enter the IP address/hostname of the remote gateway. Multiple remote gateways can be configured by separating each entry with a semicolon. If one gateway is not available, the VPN will connect to the next configured gateway.
	Port	Enter the access port. Available if *SSL VPN* is selected. The default port is 443.
	Require Certificate	Enable to require a certificate. Available if *SSL VPN* is selected.
	Authentication Method	Select the authentication method for the VPN. Available if *IPsec VPN* is selected.
	Pre-Shared Key	Enter the pre-shared key required. Available if *Pre-Shared Key* is selected for *Authentication Method*.
	Prompt for Username	Enable to prompt for the username when accessing VPN.
VPN Settings		Available if *IPsec VPN* is selected for the VPN type.
	Mode	Select *Main* or *Aggressive*.
	Options	Select *Mode Config*, *Manual Set*, or *DHCP over IPsec*.
	Specify DNS Server (IPv4)	Specify the DNS server for the VPN tunnel. Available if *Manual Set* is selected.

	Assign IP Address (IPv4)	Enter the IP address to assign for the VPN tunnel. Available if *Manual Set* is selected.
	Split Table	Enter the IP address and subnet mask for the VPN tunnel. Available if *Manual Set* or *DHCP over IPsec* is selected.
Phase 1		Available if *IPsec VPN* is selected for the VPN type. Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of two combinations. The remote peer or client must be configured to use at least one of the proposals that you define.
	Encryption	Select the encryption standard.
	Authentication	Select the authentication method.
	DH Groups	Select one or more Diffie-Hellman groups from DH group 1, 2, 5, 14, 15, 16, 17, 18, 19 and 20. At least one of the DH Group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations.
	Key Life	Enter the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The key life can be from 120 to 172,800 seconds.
	Local ID	Enter the local ID.
	Enable Implied SPDO	Enable implied SPDO. Enter the timeout in seconds.
	Dead Peer Detection	Select this checkbox to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required.
	NAT Traversal	Select the checkbox if a NAT device exists between the client and the local FortiGate unit. The client and the local FortiGate unit must have the same NAT traversal setting (both selected or both cleared) to connect reliably.
	Enable Local LAN	Enable local LAN.
	Enable IKE Fragmentation	Enable IKE fragmentation.

Phase 2		Available if *IPsec VPN* is selected for the VPN type. Select the encryption and authentication algorithms that will be proposed to the remote VPN peer. You can specify up to two proposals. To establish a VPN connection, at least one of the proposals that you specify must match configuration on the remote peer.
	Encryption	Select the encryption standard.
	Authentication	Select the authentication method.
	DH Group	Select one Diffie-Hellman (DH) group (1, 2, 5, 14, 15, 16, 17, 18, 19 or 20). This must match the DH Group that the remote peer or dialup client uses.
	Key Life	The Key Life setting sets a limit on the length of time that a phase 2 key can be used. The default units are seconds. Alternatively, you can set a limit on the number of kilobytes (KB) of processed data, or both. If you select both, the key expires when either the time has passed or the number of KB have been processed. When the phase 2 key expires, a new key is generated without interrupting service.
	Enable Replay Detection	Replay detection enables the unit to check all IPsec packets to see if they have been received before. If any encrypted packets arrive out of order, the unit discards them.
	Enable Perfect Forward Secrecy (PFS)	Select the checkbox to enable Perfect forward secrecy (PFS). PFS forces a new Diffie-Hellman exchange when the tunnel starts and whenever the phase 2 key life expires, causing a new key to be generated each time.
	Auto Keep Alive	Enable auto keep alive.
	Allow non-administrators to use machine certificates	Enable to allow non-administrator users to use local machine certificates.
Advanced Settings		
	Enable One-Time Password	Enable one-time password.
	Enable XAuth	Enable XAuth.
	Prompt for Certificate	Enable to prompt the user for the certificate.
	Enable Single User Mode	Enable Single User Mode.
	Show Passcode	Enable to remember your password.
	Save Username	Enable to save your username.

	Show "Remember Password" Option	Enable to have the VPN tunnel remember the password.
	Show "Always Up" Option	Enable to have the VPN tunnel always up. This also needs to be enabled on the FortiGate.
	Show "Auto Connect" Option	Enable to automatically connect the VPN tunnel. This also needs to be enabled on the FortiGate.
	On Connect Script	Enable the on connect script. Enter your script. This also needs to be enabled on the FortiGate.
	On Disconnect Script	Enable the disconnect script. Enter your script. This also needs to be enabled on the FortiGate.

Vulnerability Scan

Configuration		Description
Vulnerability Scan		Enable or disable Vulnerability Scan.
Scan on Registration		Scan endpoints upon connecting to a FortiGate.
Scan on Vulnerability Signature Update		Scan endpoints upon updating a vulnerability signature.
Scan for OS Updates		Scan for OS updates.
Enable Proxy		Enable proxy.
Scheduled Scan		Configure settings for scheduled scanning.
	Schedule Type	Configure either *Daily*, *Weekly*, *Monthly*.
	Scan On	Configure the day the scan will run (1st-31st of the month). This only applies if the schedule type is configured to *Monthly*.
	Start At	Configure the time the scan will start.
Automatic Patching		
	Patch Level	When enabled, patches are installed automatically when vulnerabilities are detected. Select one of the following: • Critical: Patch critical vulnerabilities only • High: Patch high severity, and above, vulnerabilities • Medium: Patch medium severity, and above, vulnerabilities • Low: Patch low severity, and above, vulnerabilities • All: Patch all vulnerabilities. Automatic patching may require endpoint reboot.
Exclusions		

Configuration		Description
	Exempt Application Vulnerabilities Requiring Manual Update from Vulnerability Compliance Check	When enabled, all applications that require the endpoint user to manually patch vulnerabilities are excluded from vulnerability compliance check. Even if compliance is enabled for FortiClient in managed mode and FortiGate compliance rules require it, manual software patches required for application vulnerabilities do not need to be installed within the specified time frame to maintain compliant status and network access. This option does not exclude applications from vulnerability scanning.
	Exclude Selected Applications from Vulnerability Compliance Check	In the *<number> Applications* list, click the applications to exclude from vulnerability compliance check, and they are automatically moved to the *<number> Excluded Applications* list. In the *<number> Excluded Applications* list, click the applications to remove from the exclusion list. Applications on the exclusion list are exempt from needing to install software patches within the timeframe specified in FortiGate compliance rules to maintain compliant status and network access. Applications on the list are not excluded from vulnerability scanning.
	Disable Automatic Patching for These Applications	Disable automatic patching for the applications excluded from vulnerability compliance check.

System Settings

The majority of these configuration options are only available for Windows, Mac, and Linux profiles. Options available for Chromebook profiles, such as *Upload Logs to FortiAnalyzer/FortiManager*, are indicated as such in the table below.

Some options are only available when *Advanced* view is enabled.

Configuration		Description
UI		Specify how the FortiClient user interface appears when installed on endpoints.
Show Dashboard Banner		Enable the dashboard banner.
Require Password to Disconnect from EMS		Turn on the password lock for FortiClient.
	Password	Type a password.
Do Not Allow User to Back Up Configuration		Enable to not allow users to back up configuration.
Hide System Tray Icon		Enable to hide the system tray icon.

Configuration	Description
Language	Configure the language used by the FortiClient Console. The default is the system operating language. Select one of the following: • os-default • zh-tw • cs-cz • de-de • en-us • fr-fr • hu-hu • ru-ru • ja-jp • ko-kr • pt-br • sk-sk • es-es • zh-cn • et-ee • lv-lv • lt-lt • fi-fi • sv-se • da-dk • pl-pl • nb-no
Log	Specify FortiClient log settings.
Level	This option is available for Chromebook profiles. Generates logs equal to or more critical than the selected level. Select one of the following: • Disabled • Emergency: The system becomes unstable. • Alert: Immediate action is required. • Critical: Functionality is affected. • Error: An error condition exists and functionality could be affected. • Warning: Functionality could be affected. • Notice: Information about normal events. • Info: General information about system operations. • Debug: Debug FortiClient.

Configuration		Description
Features		Select features for which logs will be generated: • AntiVirus • Application Firewall • Telemetry • FSSOMA • Proxy • IPsec VPN • SSL VPN • Update • Vulnerability • Web Filter • Sandbox
Client-Based Logging When On-Net		Include local log messages when FortiClient is on-net. For information about the onnet feature, see the *FortiClient Administration Guide*.
Upload Logs to FortiAnalyzer/FortiManager		This option and all nested options are available for Chromebook profiles. Turn on to configure endpoints to sends logs to the FortiAnalyzer or FortiManager device at the specified address or hostname.
	Upload Traffic Logs	Enable to upload traffic logs.
	Upload Vulnerability Logs	Enable to upload vulnerability logs to FortiAnalyzer.
	Upload Event Logs	Enable to upload event logs.
	IP Address/Hostname	Enter the IP address or hostname/FQDN. With Chromebook profiles, when connecting to FortiAnalyzer 5.6+, use the format *https://FAZ-IP:port/logging*. Otherwise, use the format *https://FAZ-IP/jsonrpc/fazapi/logs*. If using a port other than the default, use <address>:<port>.
	SSL Enabled	Enable SSL.
	Upload Schedule (minutes)	Configure the upload schedule in minutes.
	Log Generation Timeout (seconds)	Configure the log generation timeout in seconds.
	Log Retention (days)	Configure the duration of time to retain logs in days.
	Compress Logs	Enable to compress logs.
Proxy		

Configuration		Description
Use Proxy for Updates		Enable to access FortiGuard using the configured proxy.
	Connect to FDN Directly If Proxy Is Offline	Enable to connect to FDN directly if proxy is offline.
Use Proxy for Virus Submission		Enable to use the configured proxy to submit viruses to FortiGuard.
	Type	Configure the type. Options include: • http • socks4 • socks5
	IP Address/Hostname	Enter IP address/hostname.
	Port	Enter the port number.
	Username	Enter the username.
	Password	Enter the password. Enable Show Password to show the password in plain text.
Update		Specify whether to use FortiManager to update FortiClient on endpoints
Use FortiManager for Client Software/Signature Update		Turn on to enable FortiClient EMS to obtain antivirus signatures and software updates from the FortiManager device at the specified IP address or hostname.
	IP Address/Hostname	Enter the IP address/hostname.
	Port	Enter the port number.
	Failover Port	Enter the failover port.
	Timeout	Enter the timeout interval.
	Failover to FDN When FortiManager Is Not Available	Enable failover to FDN when FortiManager is not available.
Software Update		Enable to update FortiClient software on endpoints.

Configuration		Description
	Update Action	Select the option to implement when new software updates are available: • Notify Only The Update Action will be set to *Disabled*. The Advanced XML configuration should be: `<update_action>disable</update_action>` • Download And Install • Download Only
Scheduled Updates		Enable to configure the update schedule.
	Schedule Type	Select *Interval* or *Daily* for your schedule time.
	Update Every	Configure the interval.
FortiProxy		Enable FortiProxy (disable only when troubleshooting). You must enable FortiProxy to use the Web Filter options as well as some AntiVirus options.
HTTPS Proxy		Enable HTTPS proxy. If disabled, FortiProxy no longer inspects HTTPS traffic.
	HTTP Timeout	Enter the HTTP timeout interval.
POP3 Client Comforting		Enable POP3 client comforting.
POP3 Server Comforting		Enable POP3 server comforting.
SMTP Client Comforting		Enable SMTP.
Self Test		Enable Self Test. You have the option to *Notify* the *Last Port*.
	Notify	Enable Notify and enter the last port.
	Last Port	Last port number.
Endpoint Control		Specify settings for the endpoints.
Show Bubble Notifications		Enable to show bubble notifications.
Show Profile Details		Enable to show profile details.
Silent Registration		Turn on to enable silent connection of endpoints, which means that endpoints are connected without user interaction. Turn off to require user interaction to connect endpoints.
Log off When User Logs Out of Windows		Turn on to log off FortiClient when the endpoint user logs out of Windows. Turn off to remain logged in.
Disable Unregister		Turn on to forbid users from disconnecting FortiClient from FortiClient EMS. Turn off to allow users to disconnect FortiClient from FortiClient EMS.

Configuration		Description
	Disable FortiGate Switch	Enable to disable FortiGate switch.
Hide Compliance Enforcement Feature Message from Compliance Tab		Enable to hide the compliance encoforcement feature message from the *Compliance* tab. This option is only enforced on FortiClients connected to FortiClient EMS. This option does not apply to monitored clients.
On-Net Subnets		Turn on to enable on-net subnets. For details on how FortiClient determines on-net/off-net status, see the *FortiClient Administration Guide*.
	IP Addresses/Subnet Masks	Enter IP addresses/subnet mask to connect to onnet subnets.
	Gateway MAC Address	Enable gateway MAC address.
	MAC Addresses	Enter MAC addresses.
Other		
Install CA Certificate on Client		Turn on to select and install a CA certificate on the FortiClient endpoint. You can add certificates by going to *Profile Components* > *Manage CA Certificates*.
FortiClient Single Sign-On Mobility Agent		Select to enable Single Sign-On Mobility Agent for FortiAuthenticator. To use this feature you need to apply a FortiClient SSO mobility agent license to your FortiAuthenticator device.
	IP Address/Hostname	Enter the FortiAuthenticator IP address or hostname.
	Port	Enter the port number.
	Pre-Shared Key	Enter the pre-shared key. The pre-shared key should match the key configured on your FortiAuthenticator device.
iOS		
Distribute Configuration Profile		Enable and browse for your `.mobileconfig` file to distribute the configuration profile.
Privacy		
Send Usage Statistics to Fortinet		Submit virus information to FDS.

XML Configuration

Configuration	Description
XML editor	Configure using the XML editor. See the FortiClient XML Reference Guide in the Fortinet Document Library.

Profile Components

You can manage FortiClient installers, connected FortiSandbox units, and CA certificates under *Profile Components*.

Managing installers

- FortiGuard Distribution Network on page 141
- Adding FortiClient installers on page 141
- Uploading custom FortiClient installers on page 143
- Viewing installers on page 145
- Deleting FortiClient installers on page 145

FortiGuard Distribution Network

FortiClient EMS automatically connects to FortiGuard Distribution Network (FDN) to provide access to FortiClient installers you can use with FortiClient EMS profiles. If a connection to FDN is not available, you must manually download FortiClient installers to use with FortiClient EMS. See Downloading FortiClient installers on page 141.

Downloading FortiClient installers

You can download FortiClient installers to use with FortiClient EMS from the following locations:

https://support.fortinet.com	Fortinet Customer Service & Support. Requires a support account with a valid support contract. Download the Microsoft Windows (32-bit/64-bit) or the macOS installation file.
www.forticlient.com	FortiClient homepage. Download the FortiClient online installation file. The installer file performs a virus and malware scan of the target system prior to installing FortiClient.

Adding FortiClient installers

When you add a FortiClient installer to FortiClient EMS, you can specify what FortiClient features to include in the installer for the endpoint. You can include a feature in the installer, then disable the feature in the profile. Because the feature is included in the installer, you can update the profile later to enable the feature on the endpoint.

When you add a FortiClient installer to FortiClient EMS, an installer for the Windows operating system and an installer for the macOS operating system are added to FortiClient EMS.

After you add a FortiClient installer to FortiClient EMS, you cannot edit it. You can delete the installer from FortiClient EMS, and edit the installer outside of FortiClient EMS. You can then add the edited installer to FortiClient EMS.

To add FortiClient installers:

1. Go to *Profile Components* > *Manage Installers*.
2. Click *Add*.
3. On the *General* tab, set the following options:

Name	Type the FortiClient installer's name.
Notes	(Optional) Type any notes about the FortiClient installer.
Version	Select the FortiClient version to install. Click *Upload* to add a custom FortiClient installer.
Patch version	Select the specific FortiClient patch version to install.
Keep updated to the latest patch	Select to enable FortiClient to automatically update to the latest patch release when FortiClient is installed on an endpoint. This field is only available for the latest FortiClient version FortiClient EMS can access from FortiGuard. This option is not available if an older FortiClient version is selected.

4. Click *Next*. On the *Features* tab, set the following options:

Security Fabric Agent (Mandatory Feature)	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry and Vulnerability Scanning enabled.
Secure Access Architecture Components	Enable to install FortiClient with SSL VPN and IPsec VPN enabled. Disable to omit SSL VPN and IPsec VPN support from the FortiClient installer.
Advanced Persistent Threat (APT) Components	Enable to install FortiClient with APT components enabled. Disable to omit APT components from the FortiClient installer. Includes FortiSandbox detection and quarantine features.
Additional Security Features	Enable to select one, two, or all of the following features: • AntiVirus • Web Filtering • Application Firewall • Single Sign-On mobility agent Disable to exclude the features from the FortiClient installer.

5. Click *Next*. On the *Advanced* tab, set the following options:

Enable automatic registration	Enable to configure FortiClient to automatically connect Telemetry to EMS or FortiGate after FortiClient is installed on the endpoint. Disable to turn off this feature and require endpoint users to manually connect Telemetry to EMS or FortiGate.

Enable desktop shortcut	Enable to configure the FortiClient installer to create a desktop shortcut on the endpoint.
Enable start menu shortcut	Enable to configure the FortiClient installer to create a Start menu shortcut on the endpoint.
Enable endpoint tag	Enable to configure an endpoint tag to assign to endpoints. Under *Endpoint Tag*, select an existing tag or enter a new tag. FortiClient EMS automatically groups tagged endpoints according to group assignment rules. See Group assignment rules on page 162. This option is not available when the FortiClient installer selected or uploaded in step 3 is a version prior to 6.0.0.

6. Click *Next*. On the *Telemetry* tab, set the following options:

EMS	Click *EMS* to configure the FortiClient installer to connect Telemetry to EMS.
FortiGate	Click *FortiGate*, and select the name of the gateway list to use. The gateway list defines the IP address for FortiGate and includes the IP address for EMS. You must define a FortiClient Telemetry gateway list to select FortiGate. If you have not created a list, the *No Gateway IPs have been defined* dialog box is displayed, and you can click *OK* to create a list.

7. Click *Save*. The FortiClient installer is added to FortiClient EMS and displays on the *Manage Installers* pane.

If the *Sign software packages* option is enabled in *System Settings* > *Server*, Windows installers display as being from the publisher specified in the certificate file. See Configuring Server settings on page 167.

Uploading custom FortiClient installers

You can create a custom FortiClient installer and add it to FortiClient EMS. Alternately, if a connection to FDN is not available, you may need to manually download a FortiClient installer and add it to FortiClient EMS. See FortiGuard Distribution Network on page 141.

The online installer available for download at FortiClient.com cannot be uploaded into the *Add Installer* dialog in *Manage Installers*.

To add custom FortiClient installers to FortiClient EMS:

1. Download a FortiClient installer. See Downloading FortiClient installers on page 141.
2. Go to *Profile Components* > *Manage Installers*.
3. Click *Add*. The *Add Installer* dialog box displays.

4. On the *General* tab, set the following options:

Name	Type the FortiClient installer's name.
Notes	(Optional) Type any notes about the FortiClient installer.

5. In the *Version* list, select *Upload*. Uploading options display.
6. Set the following options:

Upload Windows Installers	Enable to upload FortiClient installers for the Windows operating system.
Windows 64-bit installer	Click the *Browse* button to locate and select a custom 64-bit installer for the Windows operating system.
Windows 32-bit installer	Click the *Browse* button to locate and select a custom 32-bit installer for the Windows operating system.
Upload Mac OS X Installers	Enable to upload a FortiClient installer for the macOS operating system.
Mac OS X installer	Click the *Browse* button to locate and select a custom installer for the macOS operating system.

7. On the *Advanced* tab, set the following option:

Enable endpoint tag	Enable to configure an endpoint tag to assign to endpoints. Under *Endpoint Tag*, select an existing tag or enter a new tag. FortiClient EMS automatically groups tagged endpoints according to group assignment rules. See Group assignment rules on page 162. This option is not available when the FortiClient installer selected or uploaded in step 3 is a version prior to 6.0.0.

8. On the *Telemetry* tab, set the following options:

EMS	Click *EMS* to configure the FortiClient installer to connect Telemetry to EMS.
FortiGate	Click *FortiGate*, and select the name of the gateway list to use. The gateway list defines the IP address for FortiGate and includes the IP address for EMS. You must define a FortiClient Telemetry gateway list to select FortiGate. If you have not created a list, the *No Gateway IPs have been defined* dialog box displays, and you can click *OK* to create a list.

9. Click *Save*. The installer is added to FortiClient EMS and displays on the *Manage Installers* pane.

If the *Sign software packages* option is enabled in *System Settings* > *Server*, Windows installers display as being from the publisher specified in the certificate file. See Configuring Server settings on page 167.

Viewing installers

After you add FortiClient installers to FortiClient EMS, you can view them on the *Manage Installers* pane.

To view FortiClient installers:

1. Go to *Profile Components* > *Manage Installers*.
   The *Manage Installers* pane displays available installers.

Available Installers	Lists the following information about each installer: • Operating system (Windows or macOS) • Version of FortiClient software • Whether Auto Update is enabled or disabled • Name of the FortiClient installer • Location of the FortiClient installer FortiClient EMS. Endpoint users can access this location to download and install FortiClient on endpoints.
View Details	Lists the following information about the selected installer: • Name of the FortiClient installer • Operating system (Windows and/or macOS) • Version of FortiClient software • Enabled features • Managed by FortiGate or FortiClient EMS • Telemetry connection IP address • Auto update enabled/disabled • Desktop shortcut enabled/disabled • Start menu shortcut enabled/disabled • Notes included when creating the installer
Turn on/offf Auto Update	Click to enable or disable auto update. When auto update is enabled, FortiClient EMS automatically keeps the installer updated to the latest patch.
Delete	Click to delete the FortiClient installer.
Add	Click to add a FortiClient installer.
Refresh	Click to refresh the FortiClient installer list.

Deleting FortiClient installers

To delete FortiClient installers:

1. Go to *Profile Components* > *Manage Installers*.
2. Click the desired installer, then click the *Delete* button.
   A confirmation dialog box displays.
3. Click *Yes*.
   The FortiClient installer is deleted from FortiClient EMS.

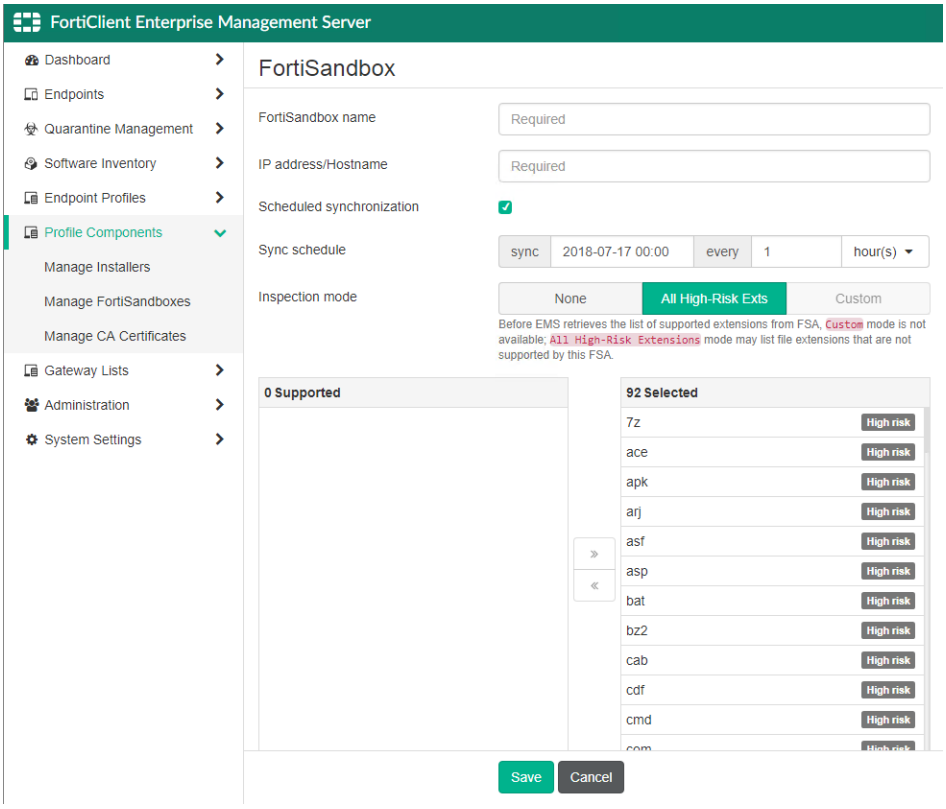
Managing FortiSandbox units

On the *Manage FortiSandboxes* pane, you can add, view, and edit FortiSandbox units, including configuring the synchronization schedule between FortiClient EMS and FortiSandbox. FortiSandbox units configured on the *Manage FortiSandboxes* pane can be selected from the *Sandbox Detection* tab when creating or editing an endpoint profile. See Sandbox Detection on page 122.

Adding a FortiSandbox

1. Go to *Profile Components* > *Manage FortiSandboxes*.
2. Click *Add*.
3. In the *FortiSandbox name* field, enter the desired name for the FortiSandbox. This name appears on the *Manage FortiSandboxes* pane and on the *Sandbox Detection* tab when configuring an endpoint profile.
4. In the *IP address/Hostname* field, enter the FortiSandbox's IP address or hostname.
5. If desired, select the *Scheduled synchronization* checkbox. If *Scheduled synchronization* is not enabled, you can only sync FortiSandbox configuration by clicking *Sync Now* on the *Manage FortiSandboxes* pane.
6. If *Scheduled synchronization* was selected, configure the sync schedule in days, hours, or minutes.
7. Under *Inspection mode*, select one of the following:
   a. *None*: FortiSandbox does not inspect any files to FortiSandbox.
   b. *All High-Risk Exts*: FortiClient inspects all supported high-risk file extensions and sends to FortiSandbox as appropriate. The list displayed may include file extensions not supported by the FortiSandbox unit.
   c. *Custom*: Only available after FortiClient EMS retrieves the list of supported file extensions from the FortiSandbox unit. Customize the list of selected file extensions to inspect.

8. Click *Save*.

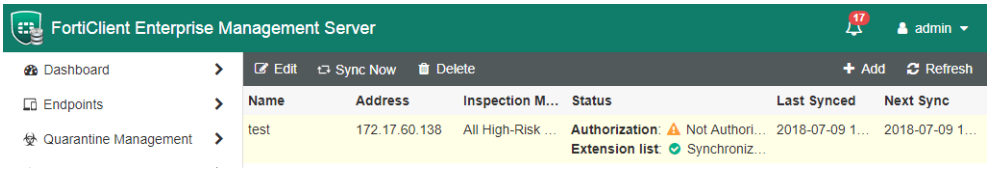


Editing a FortiSandbox

1. Go to *Profile Components* > *Manage FortiSandboxes*.
2. Select the desired FortiSandbox.
3. Click *Edit*.
4. Edit the configuration as desired.
5. Click *Save*.

Viewing FortiSandboxes

1. Go to *Profile Components* > *Manage FortiSandboxes*.



The list of configured FortiSandboxes and a toolbar display in the content pane.

Name	Name of FortiSandbox unit.

Address	IP address of FortiSandbox unit.
Inspection Mode	Configured inspection mode for file extensions: *None*, *All High-Risk Exts*, or *Custom*.
Status	Displays authorization status and extension list status: • Authorization status: connection status between FortiClient EMS and the FortiSandbox. • Extension list status: whether FortiClient EMS has the updated list of file extensions supported by the FortiSandbox.
Last Synced	Time of last sync between FortiClient EMS and the FortiSandbox.
Next Sync	Time of next scheduled sync (if any) between FortiClient EMS and FortiSandbox.

Deleting a FortiSandbox

1. Go to *Profile Components* > *Manage FortiSandboxes*.
2. Select the desired FortiSandbox.
3. Click *Delete*.
4. Click *Yes*. Note you can only delete the profile if it is not assigned to or used in an endpoint profile.

Managing CA certificates

You can upload or import CA certificates into FortiClient EMS.

Uploading certificates

You can locally upload a CA certificate.

To upload a certificate:

1. Go to *Profile Components* > *Manage CA Certificates*.
2. Select *Upload*.
3. In the *Upload Local Certificate* window, click *Browse* and locate the certificate.
4. Click *Upload*.

Importing certificates

To import certificates:

1. Go to *Profile Components* > *Manage CA Certificates*.
2. Select *Import*.

3. In the *Import Certificates from FortiGate* window, enter the following information:

IP address/Hostname	Enter the server IP/hostname in the following format: `<ip address> : <port>`.
VDOM	Enter the VDOM.
Username	Enter the username.
Password	Enter the password.

4. Click *Import* to import the certificate.

Gateway Lists

Gateway lists are useful when using FortiClient EMS integrated with FortiGate. If using FortiClient EMS without FortiGate, you are not required to use gateway lists.

You can use gateway lists to specify what IP addresses or fully qualified domain names (FQDN) and ports endpoints can use to connect FortiClient Telemetry to FortiGate, EMS, or FortiGate and EMS. You can create one or more gateway lists and assign them to domains or workgroups.

After deploying FortiClient to endpoints, FortiClient uses the gateway list to try and connect FortiClient Telemetry to FortiGate or EMS. This connection is based on the gateway list received from EMS.

Even if the endpoint is already connected to a FortiGate, you can still assign a gateway list to endpoints. You can also update existing gateway lists as required. The updates are pushed to endpoints with the next Telemetry communication.

Creating gateway lists

Gateway lists are useful when using FortiClient EMS integrated with FortiGate. If using FortiClient EMS without FortiGate, you are not required to use gateway lists.

You can create one or more gateway lists. Each list can contain IP addresses for multiple FortiGate units.

To create gateway lists:

1. Go to *Gateway Lists* > *Manage Gateway Lists*.
2. Click the *Add* button.

3. Configure the following:

Name		Enter the list name.
Comment		Enter additional comments (optional).
IP addresses/hostnames		Enter the IP address and port for FortiGate devices using the following format: IP:port. You can also use an FQDN. Press the *Enter* key to add additional IP addresses.
Connect to local subnets only		Enable to only allow to connect to local subnets.
Use connection key		Enable the connection key endpoints can use to connect to FortiGate units.
	New connection key	Enter the connection key.
	Confirm new connection key	Reenter the connection key to confirm.
Managed by EMS		Select an option from the dropdown list. Users can configure this IP address in *System Settings* > *Server*.

4. Click *Save*.

Exporting gateway lists to XML

After you create and save a gateway list, the *Export XML* button displays, and you can export the list to a configuration file in XML format.

To export Gateway lists to XML:

1. Go to *Gateway Lists* > *Manage Gateway Lists*.
2. Click a list.
3. Click the *Export* button.

   A `<filename>.conf` file is downloaded to your computer. Following is an example of the XML:

```
<?xml version="1.0" encoding="utf-8"?>
<forticlient_configuration>
   <endpoint_control>
      <fortigates>
         <fortigate>
            <name>FortiGate</name>
            <registration_password></registration_password>
            <addresses>1.1.1.1:8013</addresses>
         </fortigate>
      </fortigates>
      <notification_server>
         <registration_password></registration_password>
         <address>1.1.1.1:8013</address>
      </notification_server>
   </endpoint_control>
```

```
</forticlient_configuration>
```

Viewing gateway lists

When you create gateway lists, they are listed under *Gateway Lists* in the left pane. You can view the gateway lists and their settings.

To view gateway lists:

1. Under *Gateway Lists*, click the desired gateway list to display it in the content pane.

Assigning gateway lists to endpoints

After creating a gateway list, you can assign the list to endpoints. When you assign the IP list and FortiClient Telemetry data connection process has started, the endpoint connects to a FortiGate or EMS, based on the gateway list.

To assign gateway lists to endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Assign gateway list*.
3. Select the desired list or create a new gateway list.

Viewing assigned gateway lists

To view assigned gateway lists:

1. Select an endpoint.
2. View *Summary* > *Configuration* > *IP List*.

Deployment

You can use FortiClient EMS to deploy FortiClient on endpoints that are part of an Active Directory (AD) server. Note this is not applicable to Chromebooks. Deploying FortiClient from FortiClient EMS requires the following steps:

- Preparing the AD server for deployment
- Deploying FortiClient on endpoints

After FortiClient is deployed on endpoints, and endpoints are connected to FortiClient EMS, you can update endpoints by editing the associated profiles.

You can also use FortiClient EMS to uninstall and upgrade FortiClient on endpoints that are part of an AD server.

You cannot use workgroups to deploy an initial installation of FortiClient to endpoints. However, after FortiClient is installed on endpoints and endpoints connect to FortiClient EMS, you can use workgroups to uninstall and update FortiClient on endpoints.

You cannot use FortiClient EMS to deploy an initial installation of FortiClient (macOS) to endpoints. However, after FortiClient (macOS) is installed on endpoints and endpoints connect to FortiClient EMS, you can use FortiClient EMS to uninstall and update FortiClient (macOS) on endpoints.

Preparing the AD server for deployment

Before you can successfully deploy a FortiClient installation, ensure you install and prepare the AD server as follows.

- Configure a group policy on the AD server.
- Configure the required Windows services on the AD server.
- Create deployment rules for Windows firewall.
- Configure Windows firewall domain profile settings.

Configuring a group policy on the AD server

To configure a group policy on the AD server:

1. On the AD server, open *Group Policy Management*.
2. Right-click the *Default Domain Policy* setting. The Group Policy Management Editor opens.

   A new policy is applied to the entire AD domain. Alternatively, you can create a new Group Policy Object, and link it to one or more organizational units (OU) in the AD server that contains the endpoint computers on which FortiClient will be deployed.

Configuring required Windows services

To configure required Windows services:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration* > *Policies* > *Windows Settings* > *Security Settings* > *System Services*.
2. In the right panel, select the following:
   a. Task Scheduler: Automatic
   b. Windows Installer: Manual
   c. Remote Registry: Automatic

Creating deployment rules for Windows firewall

To create deployment rules for Windows firewall:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration* > *Policies* > *Windows Settings* > *Security Settings* > *Windows Firewall with Advanced Security* > *Inbound Rules*.
2. Right-click *Inbound Rules* and select *New Rule*.
3. Select *Predefined* from the dropdown list and select *File and Printer Sharing*.
4. Click *Next*.
5. Ensure that the *File and Printer Sharing (SMB-In)* box is selected and click *Next*.
6. Select *Allow the connection* and click *Finish*.
7. Repeat steps 1 to 2.
8. Select *Predefined* from the dropdown list and select *Remote Scheduled Tasks Management* and click *Next*.
9. Ensure that the *Remote Scheduled Tasks Management (RPC)* box is checked and click *Next*.
10. Select *Allow the connection* and click *Finish*.

Configuring Windows firewall domain profile settings

To configure Windows firewall domain profile settings:

1. In the Group Policy Management Editor, in the left panel, go to *Computer Configuration* > *Policies* > *Administrative Templates* > *Network* > *Network Connections* > *Windows Firewall* > *Domain Profile*.
2. Select *Allow inbound file and printer sharing* exception:
   a. Right-click and select *Edit*.
   b. Enable the radio button.
   c. Provide the EMS server's IP address in the text box.
   d. Allow unsolicited incoming messages from these IP addresses.
   e. Click OK.
3. Select *Allow inbound remote administration* exception.

   Repeat steps listed in step 2 above to create an exception.
4. Select *Allow ICMP Exceptions*:
   a. Right-click and select *Edit*.
   b. Enable the radio button.

c. Select the *Allow inbound echo request* checkbox.
d. Click *OK*.

To deploy the group policy manually, execute `gpupdate /force` on the AD server to update the group profile on all endpoints.
Execute `gpresult.exe /H gpresult.html` on any AD client to view the group policy deployed on the endpoints.

Preparing Windows endpoints for FortiClient deployment

The following services must be enabled and configured on each Windows endpoint before FortiClient is deployed to them:

- Task Scheduler: Automatic
- Windows Installer: Manual
- Remote Registry: Automatic

The Windows Firewall must be configured to allow the following inbound connections:

- File and Printer Sharing (SMB-In)
- Remote Scheduled Tasks Management (RPC)

For AD group deployments, an AD administrator account is required. For non-AD deployments, the installer URL can be shared with users, who can then download and install FortiClient manually. You can locate the installer URL in *Manage Installers*. Go to *Profile Components* > *Manage Installers*.

Deploying FortiClient on endpoints

Before you can successfully deploy a FortiClient installation from FortiClient EMS using an AD server, you must have prepared the AD server. See Preparing the AD server for deployment on page 153.

To deploy FortiClient by using AD servers

1. Add the AD server to FortiClient EMS by adding a domain. See Adding endpoints using an Active Directory domain server on page 77.
2. Add a FortiClient installer package to FortiClient EMS. See Adding FortiClient installers on page 141.
3. Add a profile, select the FortiClient installer package, and configure FortiClient features in the profile. See Creating profiles to deploy FortiClient on page 105.
4. Assign the profile to a branch of the AD domain to push the FortiClient installation process on the endpoints. See Assigning profiles on page 115.
5. Verify the deployment by monitoring FortiClient connections to the FortiClient EMS.

Deploying initial installations of FortiClient (macOS)

FortiClient EMS cannot be used to deploy initial installations of Forticlient (macOS). You can deploy an initial installation of FortiClient (macOS) by doing one of the following:

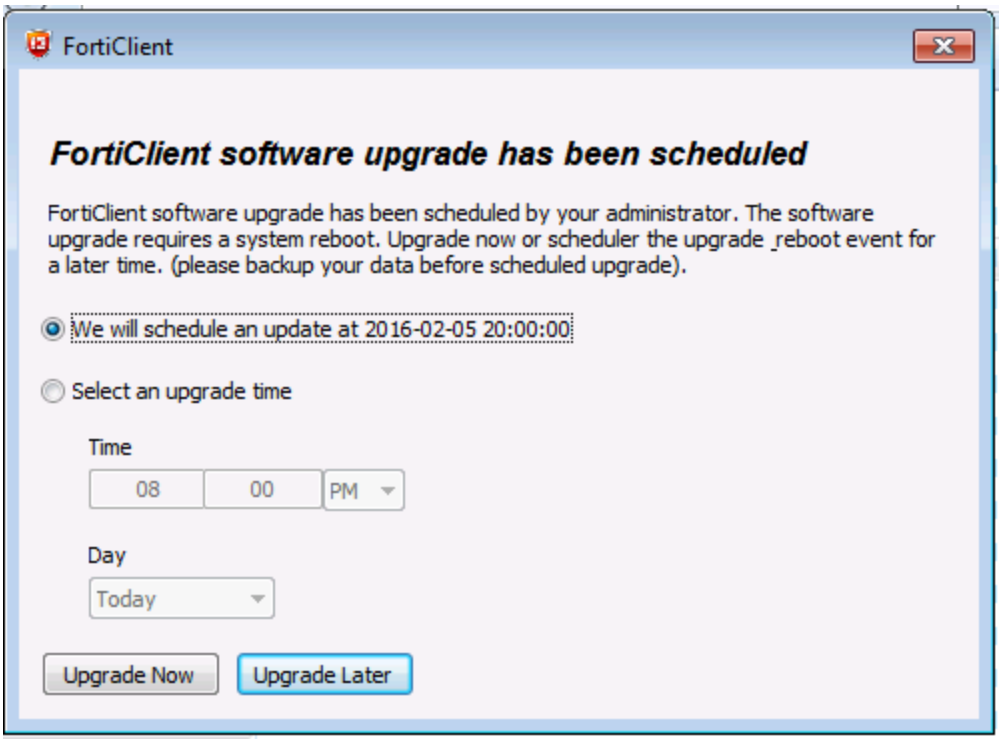
- Create a custom FortiClient (macOS) installer on FortiClient EMS with the EMS IP address embedded. Send the installer download link to users so they can install FortiClient manually on the endpoint. Once installed, FortiClient (macOS) automatically connects to FortiClient EMS and supports future deployments from FortiClient EMS directly. It is recommended to enable compliance on the FortiGate (set as warning) and put the installer download link so users can download it from the captive portal.
- Use a third party application to perform initial deployment of FortiClient (macOS) to endpoints.

After FortiClient (macOS) is installed on endpoints and has connected FortiClient Telemetry to FortiClient EMS, you can use FortiClient EMS to replace, upgrade, and uninstall FortiClient (macOS).

Deploying FortiClient upgrades from EMS

You can deploy a FortiClient software update from EMS. A prompt appears on the FortiClient endpoint when an installer package is requested to be deployed. The prompt requests the user to do one of the following:

1. Upgrade Now
   If this option is selected, it performs the upgrade and automatically restarts your computer.
2. Upgrade Later
   If this option is selected, you can indicate the time to start the upgrade. The default is 8:00 PM. Your computer automatically restarts after the upgrade has finished.



3. No Option

   If no option is selected, the upgrade occurs by default at 8:00 PM.

   After FortiClient EMS uninstalls the previous version, it asks if the user wants to reboot. The prompt requests the user to do one of the following:

   a. Reboot Now

      Select this option to have the reboot occur immediately.

   b. Reboot Later

      Select this option to indicate the time to reboot.

   c. Cancel Reboot

      Select this option to cancel the reboot request and reboot at your discretion.

Administration

Administrators

This section describes the default user accounts and permissions for FortiClient EMS. It also describes how to change the administrator password and configure Windows users.

Default user account and permissions

The default user named *admin* has complete access to all FortiClient EMS permissions, including modification, user permissions, approval, discovery, and deployment.

The *admin* user has access to all configured Windows and LDAP servers and users and has the authority to configure user privileges and permissions. If you are not authorized for certain tasks or devices, the related menu items, items in content pages, and buttons are hidden or disabled. In addition, a message informs you that you do not have permission to view the selected information or perform the selected operation.

Viewing users

You can view the default *admin* user and all users added to FortiClient EMS.

To view users:

1. Go to *Administration* > *Administrators*.
   The following information displays:

Add	Add a new user.
Refresh	Refresh the list of users.
Name	The username.
Type	Type of user.
Permissions	Type of user access.

Configuring Administrators

The following configuration options are available under *Administrators*.

Changing the admin password

By default, the *admin* user account has no password. You should add a password to increase security.

To change the admin password:

1. Go to *Administration* > *Administrators*.
2. Select the *admin* account.
3. Click *Change Password* from the toolbar. Change your password.
4. Click *Save*.

Configuring Windows user accounts

You can configure Windows users to have no access or administrator access to FortiClient EMS.

The Windows users list is derived from the host server on which FortiClient EMS is installed. If you want to add more Windows users, you must add them to the host server.

To configure Windows users:

1. Go to *Administration* > *Administrators*.
2. Click the *Add* button from the toolbar.
3. From the *User* dropdown list, select the Windows user. You can also search for the desired user by entering the user name in the *User* list search field.
4. Perform one of the following actions:
   a. Select the specific domain access for the user. See Default user account and permissions on page 158.
   b. Configure the permissions. See Administrators reference on page 159.
5. Click *Save*.

Configuring LDAP user accounts

The list of LDAP users is derived from those in the AD domain imported into EMS using *Administration* > *User Server*. If you want to add more LDAP users, they must already exist in the AD domain configured as the user server.

To configure LDAP users:

1. Go to *Administration* > *Administrators*.
2. Click the *Add* from the toolbar.
3. From the *User* dropdown list, select the LDAP user. You can also search for the desired user by entering the user name in the *User* list search field.
4. Perform one of the following actions:
   a. Select the specific domain access for the user. See Default user account and permissions on page 158.
   b. Configure the permissions. See Administrators reference on page 159.
5. Click *Save*.

Administrators reference

This section contains descriptions of the fields used to configure *Administrators*.

Following is a description of the fields in *Administration* > *Administrators* > *Add*.

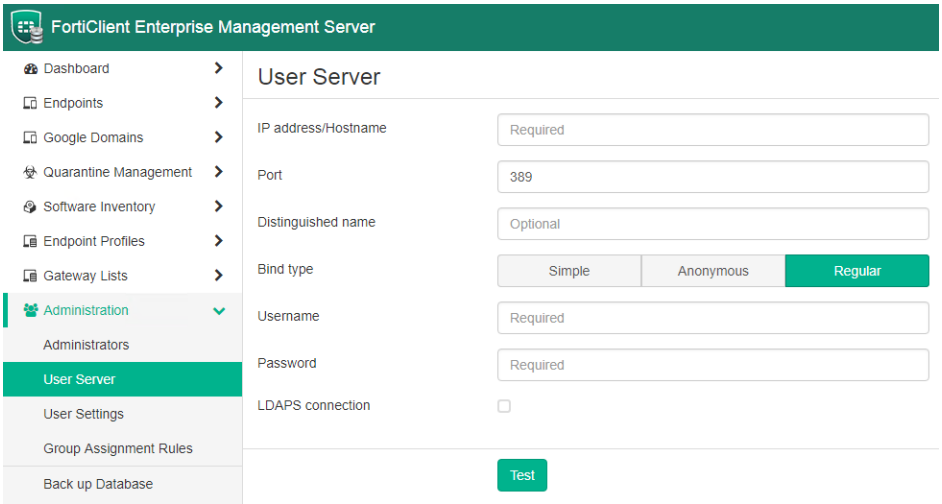
Option	Description
User	Select the Windows/LDAP user to configure permissions for FortiClient EMS.
Super Administrator permissions	Enable the super administrator feature to give the new Windows/LDAP user super administrator permissions.
Comment	Enter optional comments/information for the Windows/LDAP user.
Domain Access	Select or add access to a domain for the Windows/LDAP user and configure their permissions. If you choose one or more domains in the domain access field, you must select specific permissions.
Google Domain Access	Select or add access to a domain for the Windows/LDAP user and configure their permissions. If you choose one or more domains in the domain access field, you must select specific permissions.
General Permissions	Use the settings to configure permissions to FortiClient EMS for the selected Windows/LDAP user.
Create/Update/Delete LDAPs	Select to allow the Windows user to create, delete, and update LDAP records. Clear to disable this permission.
Create/Update/Delete custom groups	Select to allow the Windows user to create, update, and delete custom groups. Clear to disable this permission.
Create/Delete filters	Select to allow the Windows user to create and delete filters. Clear to disable this permission.
Endpoint Permissions	Use the following options to configure permissions for the selected Windows user.
Block/Unblock/Quarantine/Unquarantine/Reregister endpoints	Select to allow the Windows user to block, unblock, disconnect, quarantine, unquarantine, and reconnect endpoints. Clear to disable this permission.
Run commands on endpoints	Select to allow the Windows user to run commands on endpoints. Clear to disable this permission.
Access Software Management	Select to allow the Windows user to access the *Profile Components* > *Manage Installers* options. Clear to disable this permission.

Option	Description
Access CA Certificate Management	Select to allow the Windows user to access the *Profile Components* > *Manage CA Certificates* options. Clear to disable this permission.
Policy Permissions	
Assign/Unassign policies	Select to allow the Windows user to assign to endpoints and unassign profiles from domains/endpoints and manage custom groups. Clear to disable this permission.
Create/Update/Delete policies	Select to allow the Windows user to create, delete, edit, and rename profiles. Clear to disable this permission.

Configuring User Server

To add a user server:

1. Go *Administration* > *User Server*. The settings display.



2. Configure the following options:

IP address/Hostname	Enter the server IP address or name.
Port	Enter the server port.
Distinguished name	Enter a distinguished name.
Bind type	Select either *Simple*, *Anonymous* or *Regular* for the bind type.
Username	Appears only when the *Regular* bind type is selected. Enter the username.

	Password	Appears only when the *Regular* bind type is selected. Enter the password.
	Show Password	Enable to show the password.
	LDAPS connection	Enable LDAPS connection.

3. Click *Test* to check the LDAP server settings.
4. Click *Save*.

Configuring User Settings

To configure User Settings:

1. Go to *Administration* > *User Settings*.
2. Set the following option:

Inactivity timeout	Specify how long to keep inactive users logged into FortiClient EMS. When the time expires, the user is automatically logged out of FortiClient EMS. Type 0 to keep inactive users logged into FortiClient EMS indefinitely.

3. Click *Save*.

Group assignment rules

You can use group assignment rules to automatically place endpoints into custom groups based on their tag or IP address.

If a newly registered endpoint does not match any group assignment rule and belongs to an imported AD domain, the endpoint will be moved into the OU to which it belongs in the AD domain tree. If no AD domain has been imported, or the endpoint also does not belong to the imported AD domain, it will be placed into the *Other Endpoints* group.

Endpoints that are not applicable for any group assignment rule are automatically placed into the *Other Endpoints* group.

Tag group assignment rules

Creating or uploading a FortiClient 6.0 installer includes an option to specify an endpoint tag. For example, consider you want all endpoints located in your company's headquarters to be placed in the same endpoint group. You can configure a FortiClient 6.0 installer with an "HQ" tag, then deploy this installer to the desired endpoints. When the endpoints' FortiClient connects to FortiClient EMS, FortiClient EMS places them in the desired group. In this situation, the process is as follows:

1. In FortiClient EMS, create a tag group assignment rule that requires endpoints with the tag "HQ" to be placed into the HQ group. The tag's and group's names do not need to match. See Adding a tag group assignment rule on page 163.

2. Create or upload a FortiClient 6.0 installer. Specify the "HQ" tag when creating or uploading the installer. See Adding FortiClient installers on page 141 or Uploading custom FortiClient installers on page 143.
3. Deploy the installer to the desired endpoints or send the download link to the desired users.
4. The endpoints install FortiClient. When FortiClient connects to FortiClient EMS, the endpoint is placed in the HQ group.

IP address group assignment rules

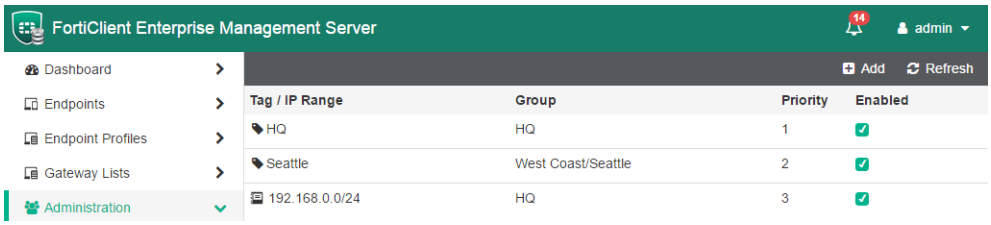
You can create a group assignment rule to automatically place all endpoints within a specified subnet or IP address range into the same custom group. In this situation, the process is as follows:

1. In FortiClient EMS, create an IP address group assignment rule that requires endpoints within a certain subnet or IP address range to be placed into the desired group. See Adding an IP address group assignment rule on page 164.
2. With the next FortiClient Telemetry communication, endpoints within the specified subnet or IP address range are placed in the specified group.

Group assignment rule priority levels

The *Priority* column on the *Group Assignment Rules* page shows the order in which group assignment rules are applied.

In the example below, consider an endpoint that is tagged "Seattle" and has an IP address that belongs to the 192.168.0.0/24 subnet. The endpoint is applicable for two rules. In this case, the endpoint is placed in the West Coast/Seattle group, since the Seattle rule has a higher priority level than the 192.168.0.0/24 subnet rule. However, if the Seattle rule is disabled, the endpoint is placed in the HQ group, as per the 192.168.0.0/24 subnet rule.



Adding a tag group assignment rule

When enabled, a tag group assignment rule automatically places endpoints with the specified tag into the specified endpoint group.

1. Go to *Administration* > *Group Assignment Rules*.
2. Click *Add*.
3. Under *Type*, select *Tag*.
4. In the *Tag* field, enter the desired tag to assign to endpoints.
5. In the *Group* field, do one of the following:
   a. If you want to place tagged endpoints into an already existing group, select the desired group from the dropdown list.

   b. If you want to place tagged endpoints into a new group, enter the desired group name. FortiClient EMS creates the new group.

      To create a new nested group, enter the desired group hierarchy. For example, to create a *Seattle* group nested under a *West Coast* group, enter *West Coast/Seattle*. FortiClient EMS then dynamically creates any group that does not exist. For example, if both the *West Coast* and *Seattle* groups do not exist, FortiClient EMS creates both groups with the desired hierarchy. If the *West Coast* group exists, FortiClient EMS creates a new *Seattle* group nested under it.

6. Enable or disable the rule by toggling *Enable Rule* on or off.
7. Click *Save*.

Adding an IP address group assignment rule

When enabled, an IP address group assignment rule requires all endpoints with an IP address in the specified subnet or IP address range to be placed into the specified endpoint group.

1. Go to *Administration* > *Group Assignment Rules*.
2. Click *Add*.
3. Under *Type*, select *IP Address*.
4. In the *Subnet/IP Range* field, enter the desired subnet or IP address range. Endpoints whose IP addresses belong to the specified subnet or IP address range will automatically be placed into the specified group.
5. In the *Group* field, do one of the following:
   a. If you want to place the endpoints into an already existing group, select the desired group from the dropdown list.
   b. If you want to place the endpoints into a new group, enter the desired group name. FortiClient EMS creates the new group.

      To create a new nested group, enter the desired group hierarchy. For example, to create a *Seattle* group nested under a *West Coast* group, enter *West Coast/Seattle*. FortiClient EMS then dynamically creates any group that does not exist. For example, if both the *West Coast* and *Seattle* groups do not exist, FortiClient EMS creates both groups with the desired hierarchy. If the *West Coast* group exists, FortiClient EMS creates a new *Seattle* group nested under it.
6. Enable or disable the rule by toggling *Enable Rule* on or off.
7. Click *Save*.

Enabling/disabling a group assignment rule

1. Go to *Administration* > *Group Assignment Rules*.
2. Select or deselect the *Enabled* checkbox for the desired group assignment rule.

Deleting a group assignment rule

1. Go to *Administration* > *Group Assignment Rules*.
2. Click the desired group assignment rule.
3. Click *Delete*.
4. In the confirmation dialog, click *Yes*.

Database management

You can back up and restore the FortiClient EMS database.

Backing up the database

To back up the database:

1. Go to *Administration* > *Back up Database*.
2. Set the following options:

Password	Type a password for backing up and restoring the database.
Confirm password	Retype the password to confirm it.

3. Click *Back up*.
   The database is backed up.

Restoring the database

To restore the database:

1. Go to *Administration* > *Restore Database*.
2. Click *Browse*.
3. Locate the database backup file, and click *Open*.
4. In the *Password* box, type the password used to back up the database.
5. Click *Restore*.
   When the database is restored, a message appears. The message instructs you to wait for the restored database to reload.
6. Wait for the restored database to be reloaded.

License upgrades or renewals

Contact Fortinet Support to upgrade or renew your FortiClient EMS license. After you have the license file, you can add it to FortiClient EMS.

To upgrade or renew the license:

1. Go to *Administration* > *Upgrade License* or *Administration* > *Upgrade License for Chromebooks*.
2. Click *Browse* and locate the license key file.
3. Click *Upload*.

Logs

You can view the log messages generated by FortiClient EMS and download raw logs.

Viewing logs

To view log messages:

1. Go to *Administration* > *Logs*.
2. Click the *Filter* icon in each column heading to apply filters.
3. Click *Clear Filters* to remove the filters.

Downloading logs

You can download the logs generated by FortiClient EMS.

To download logs:

1. Go to *Administration* > *Logs*.
2. Click *Download*.
   A zip of the raw logs is downloaded to your computer.

System Settings

This section describes FortiClient EMS settings.

Configuring Server settings

FortiClient EMS installs with a default IP address and port configured. You can change the IP address and port and configure other server settings for FortiClient EMS.

To configure Server settings:

1. Go to *System Settings* > *Server*.
2. Configure the following options under *Shared Settings*. These settings are shared between FortiClient EMS managing Windows, Mac, and Linux endpoints, and FortiClient EMS managing Chromebook endpoints:

Hostname		Displays the FortiClient EMS server's host name.
Listen on IP		Displays the IP addresses for the FortiClient EMS server. FortiClient connects to FortiClient EMS on the specified IP address.
Use FQDN		Turn on to specify a fully qualified domain name (FQDN) for the FortiClient EMS server.
	FQDN	Displayed when *Use FQDN* is turned on. Type the FQDN for the FortiClient EMS server. FortiClient can connect using the specified IP address in the *Listen on IP Addresses* option or the specified FQDN.
Remote HTTPS access		Specify settings for remote administration access to FortiClient EMS. Turn remote HTTPS access to FortiClient EMS console on and off. When enabled, type a host name in the *Custom Host Name* box to let administrators use a browser and HTTPS to log into the FortiClient EMS console. When disabled, administrators can only log into FortiClient EMS console on the server.
	Pre-defined hostname	Available when *Remote Administration HTTPS Access* is turned on. Displays the pre-defined host name. The name cannot be changed.
	Custom hostname	Available when *Remote Administration HTTPS Access* is turned on. Displays the pre-defined host name of the server on which FortiClient EMS is installed. You can customize the host name. When you change the host name, the web server restarts.
	Redirect HTTP request to HTTPS	Available when *Remote Administration HTTPS Access* is turned on. If this option is enabled, if you attempt to remotely access EMS at *http://<server_name>*, this is automatically redirected to *https://<server_name>*.

SSL certificate	Displays the SSL certificate currently imported. If you have already uploaded an SSL certificate, a *Replace* button displays.
Certificate	Browse and upload a new SSL certificate file. See Adding SSL certificates to FortiClient EMS on page 170.
Password	Configure a new SSL password.

3. Configure the following options under *EMS Settings*. These settings are used by FortiClient EMS managing Windows, Mac, and Linux endpoints:

Listen on port	Displays the default port for the FortiClient EMS server. You can change the port by typing a new port number. FortiClient connects using the specified port number.
Upload port	Displays the default port used for FortiClient to upload large amounts of data (100+ KB of data per connection) to FortiClient EMS. You can change the port by typing a new port number.

<table>
<tr><td>DHCP onnet/offnet</td><td>Enable to monitor endpoints within the company network (on-net).
Endpoints connected to FortiClient EMS from outside the company network are off-net endpoints.
There are two settings in EMS that affect the FortiClient on-net/off-net status:
1. DHCP on-net/off-net setting in EMS
2. Subnet setting in EMS
<table>
<tr><th>DHCP on-net/off-net setting</th><th>Subnet setting</th><th>DHCP 224 option</th><th>Result</th></tr>
<tr><td>Off</td><td>No</td><td>N/A</td><td>On-net</td></tr>
<tr><td>On</td><td>No</td><td>Option not configured</td><td>Off-net</td></tr>
<tr><td>On</td><td>No</td><td>Option configured</td><td>On-net</td></tr>
<tr><td>Off or on</td><td>Yes and match</td><td>Configured or not</td><td>On-net</td></tr>
<tr><td>Off or not</td><td>Yes and do not match</td><td>Configured or not</td><td>Off-net</td></tr>
</table>
Subnet values:
• no: subnet setting in EMS is disabled
• yes: subnet setting in EMS is configured
• match: client has an IP address in the configured EMS subnet
• not match: client has an IP address not in the configured EMS subnet
The following are examples on how FortiClient determines the endpoint when FortiClient is connected to EMS only. For details on how FortiClient determines on-net/off-net status in managed mode with FortiGate and FortiClient EMS, see the FortiClient Administration Guide.
• An endpoint has a status of offline when it cannot connect FortiClient Telemetry to EMS and is outside one of the on-net networks.
• An endpoint has a status of offline but on-net when it cannot connect FortiClient Telemetry to EMS but is inside one of the on-net networks.
Option 224 can have any Fortinet device's serial number. EMS assumes FortiClient is behind a FortiGate and on-net with that FortiGate.</td></tr>
<tr><td>Enable TLS 1.0/1.1</td><td>Enable TLS 1.0 and 1.1 for file downloads.
Note this option must be enabled when upgrading FortiClient on a Windows 7 device via EMS.</td></tr>
<tr><td>FortiClient download URL</td><td>FortiClient installers created in FortiClient EMS will be made available for download at the URL.</td></tr>
</table>

	Open port 10443 in Windows Firewall	Turn on to open port 10443, and turn off to close port 10443. Port 10443 is used to download FortiClient.
Sign software packages		Enable this option to have Windows FortiClient software installers created by or uploaded to EMS digitally signed with a code signing certificate.
	Timestamp server	Enter the server address to timestamp software installers with.
	Certificate	Upload the desired code signing certificate. This must be a .pfx file. After a certificate has been uploaded, its expiry date is also displayed.
	Password	Enter the certificate password. This is required for EMS to sign the software installers with the certificate.

4. If managing Chromebooks, enable *EMS for Chromebooks Settings*. You may need to restart FortiClient EMS after enabling this option.
5. Configure the following options under *EMS for Chromebooks Settings*. These settings are used by FortiClient EMS managing Chromebook endpoints:

Listen on port	Displays the default port for the FortiClient EMS server for Chromebooks. You can change the port by typing a new port number. The FortiClient Web Filter extension on Chromebooks connects to FortiClient EMS using the specified port number.
User inactivity timeout	Enter the number of hours of inactivity after which to timeout the user.
Profile update interval	Specify the profile update interval (in seconds).
Service account	Displays the service account ID currently in use.
Update service account	Update the service account with new credentials.
Reset service account	In the event your service account is broken, you can revert back to the default service account by clicking the *Reset* button. This restores the default service account. You need to *Save* the settings for the change to take effect.
ID	Available if the *Update service account* button is clicked. Enter a new service account ID.
Private key	Available if the *Update service account* button is clicked. Upload a new service account private key.

6. Click *Save*.

Adding SSL certificates to FortiClient EMS

You must add an SSL certificate to FortiClient EMS to allow HTTPS connections with the Google Admin console.

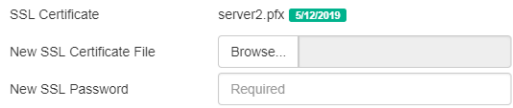
If you are using a public SSL certificate, add the certificate to FortiClient EMS. You do not need to add the certificate to the Google Admin console.

If you are not using a public SSL certificate, you must add the SSL certificate to FortiClient EMS, and the root certificate to the Google Admin console. See Adding root certificates on page 50.

To add or replace SSL certificates:

1. In FortiClient EMS, go to *System Settings* > *Server*.
2. Do one of the following:
   a. To replace an existing SSL certificate, beside *SSL certificate*, click *Update SSL certificate*.
   b. If no SSL certificate has been added yet, click the *Upload new SSL certificate* button.
3. Click *Browse* and locate the certificate file (<name>.pfx).
4. In the *Password* box, type the password.
5. Click *Test*.
6. Click *Save*.

If the SSL certificate is expiring in less than three months, the expiry date label is yellow; if it has expired, the label is red. Otherwise, it is green.



Configuring Logs settings

You can specify what level of log messages to capture in the logs for FortiClient EMS. You can also specify when to automatically delete logs and alerts.

To configure Logs settings:

1. Go to *System Settings* > *Logs*.
2. Configure the following options:

Log level	Select the level of messages to include in FortiClient EMS logs. For example, if you select *Info*, all log messages from *Info* to *Emergency* are added to the FortiClient EMS logs.
Clear logs every	Type the number of days that you want to store logs. For example, if you type 30, logs will be stored for 30 days. Any logs older than 30 days are automatically deleted.
Clear alerts every	Type the number of days that you want to keep alerts. For example, if you type 30, alerts will be kept for 30 days. Any alerts older than 30 days are automatically deleted.
Clear events every	Type the number of days that you want to keep events. For example, if you type 30, events will be kept for 30 days. Any events older than 30 days are automatically deleted.

Clear Chromebook events every	Type the number of days that you want to keep Chromebook events. For example, if you type 30, Chromebook events will be kept for 30 days. Any Chromebook events older than 30 days are automatically deleted.
Clear quarantine records older than	Enter the desired number of days. Any quarantine records older than the configured number of days are automatically deleted. The age of quarantine management records is determined by when its status was last updated.
Clear now	Click to immediately delete all FortiClient EMS logs or alerts.

3. Click *Save*.

Configuring FortiGuard settings

To configure FortiGuard settings:

1. Go to *System Settings* > *FortiGuard*.
2. Configure the following options:

Use FortiManager for client software/signature updates	Turn on to use FortiManager for updating FortiClient software or signatures. You must specify the IP address or host name for FortiManager as well as the port number.
IP address/Hostname	Enter the IP address/host name.
Port	Configure the port number.
Failover port	Configure the failover port.
Timeout	Configure the timeout interval (in seconds).
Failover	Enable failover to FDN when FortiManager is not available.

3. Click *Save*.

Configuring Endpoints settings

To configure Endpoints settings:

1. Go to *System Settings* > *Endpoints*.
2. Configure the following options:

FortiClient telemetry connection key	Add the FortiClient Telemetry connection key for FortiClient EMS. FortiClient must provide this key during connection.
Keep alive interval	Each connected FortiClient endpoint sends a short keep-alive message to FortiClient EMS at the specified interval.

Full keep alive interval	Each connected FortiClient endpoint sends a full keep-alive message to FortiClient EMS at the specified interval.
License timeout	Each connected FortiClient endpoint consumes a license seat. If an endpoint disconnects from EMS, the license seat is retained in anticipation that the endpoint will reconnect. If the endpoint does not reconnect within the given timeout, its connection record is removed from EMS. If the endpoint is removed, switched off, or becomes offline, and does not re-establish Telemetry connection to EMS within the given timeout, the endpoint is deleted from EMS even if FortiClient on the endpoint shows that it is still connected to EMS.
Automatically upload avatars	When enabled, FortiClient uploads user avatars to all FortiGate units, FortiAnalyzer units, and EMS servers it is connected to.
Allow duplicate FCT registrations	When enabled, allows duplicate FortiClient registrations by assigning the duplicate registrations new UIDs.

3. Click *Save*.

Configuring the login banner

When you enable the login banner, a message appears prior to a user logging into EMS.

To enable and configure a login banner:

1. Go to *System Settings* > *Login Banner*.
2. Click *Enable login banner*.
3. In the *Message* box, type your message. The *Preview* section displays a preview of the message.
4. Click *Save*.

Alerts

This section describes alert settings.

Configuring EMS Alerts

You can set up an SMTP server to enable alerts for EMS or endpoint events. When an alert is triggered, an email notification is sent.

To configure email alerts and an SMTP server:

1. Go to *System Settings* > *EMS Alerts*.
2. Set the following options to send an email when the following events happen:

Version Alerts		
New EMS version is available for deployment		New EMS version is available.
	Remind me everyday for 2 weeks	Enable to remind you when new EMS versions are available everyday for two weeks.
New FortiClient version is available for deployment		New FortiClient version available for deployment.
	Remind me everyday for 2 weeks	Enable to remind you when new FortiClient versions are available everyday for two weeks.
FortiClient Alerts		
EMS license is expired or about to expire		Expiring or expired EMS license.
EMS fails to sync with LDAP domains		EMS does not sync with LDAP domains.
Less than 10% of client licenses are left		Enable to be notified when there are less than 10% of client licenses left.
Client licenses have run out		Enable to be notified when you run out of client licenses.
FortiClient for Chromebook Alerts		
EMS license for Chromebooks is expired or about to expire		Expiring or expired EMS license for Chromebooks.
Less than 10% of the client licenses for Chromebooks are left		Enable to be notified when there are less than 10% of client licenses left for Chromebooks.
Client licenses for Chromebooks have run out		Enable to be notified when you run out of client licenses for Chromebooks.

3. Click *Save*.

   If you have not already set up an SMTP server, the GUI automatically prompts you to configure SMTP server settings. See Configuring SMTP Server settings on page 175.

Configuring Endpoints Alerts

To configure Endpoints Alerts:

1. Go to *System Settings* > *Endpoint Alerts*.
2. From the *Send an email every…* dropdown list, select the frequency to send emails.
3. Select the events to send emails for:
   a. Malware is detected
   b. Repeated malware is detected (same malware is detected on the same machine within the last 24 hours)
   c. Multiple malwares are detected (different malwares are detected on the same machine within the last 24 hours)
   d. Malware outbreak is detected (same malware is detected on different endpoints within the last 24 hours)
   e. Zero-day malware is detected by FortiSandbox
   f. C&C attack communication channel is detected
   g. Critical vulnerability is detected
   h. Endpoint FortiClient Telemetry is manually disconnected by user
   i. Endpoint signature database is out-of-date
   j. Endpoint software is out-of-date
   k. Endpoint is not compliant

Configuring SMTP Server settings

You can set up an SMTP server to enable alerts for EMS events. When an alert is triggered, an email notification is sent.

To configure SMTP Server settings:

1. Go to *System Settings* > *SMTP Server*.
2. Set the following options:

Server		Enter the SMTP server.
Port		Enter the port number.
Security		Select *None*, *STARTTLS*, or *SMTPS* for the security type, or select the *Auto Detect* button to automatically select the security type. If *STARTTLS* or *SMTPS* is selected, the *Username* and *Password* boxes become available.
	Username	Enter the username.
	Password	Enter the password.
From		Enter the email address to send the alerts from.
Reply-To		Enter the email address to send the replies to.
Subject		The sent e-mail alert's subject.

Recipients	Enter email address(es) to send alerts to. Click the + button to add more email addresses.
Test subject	Test email's subject.
Test message	Test email's message.
Test recipient	Email address to send the test email to.
Send Test Email	Click the button to test the configured email settings.

3. Click *Save*.

Viewing Alerts

You can view alerts FortiClient EMS generates. Examples of events that generate an alert include:

- New version of FortiClient is available
- FortiClient deployment failed
- Failure to check for signature updates
- Error encountered when downloading AD server entries
- Error encountered when scanning for local computers

A red label is associated with the *Alert* icon when new notifications are available or received. It is cleared when you view the alert.

To view alerts:

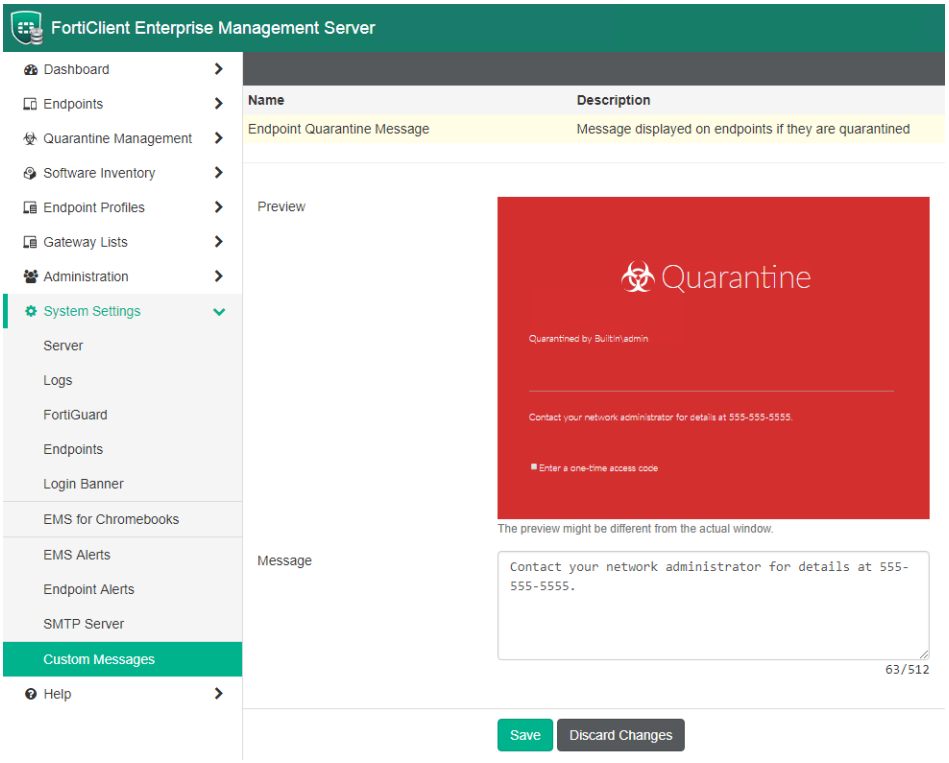
1. Click the *Alert* icon (a bell) in the toolbar.
2. Click the *Filter* icon in each column heading to apply filters.
3. Click *Clear Filters* to remove the filters.

Customizing the endpoint quarantine message

You can customize the message that displays on an endpoint when it has been quarantined by FortiClient EMS. For example, you can customize the message to include your organization's help desk phone number. This feature is only supported for endpoints running FortiClient 6.0.0 and later versions.

1. Go to *System Settings* > *Custom Messages*.
2. Select *Endpoint Quarantine Message*.
3. In the *Message* field, enter the desired message. You can enter up to 512 characters. The *Preview* section displays the custom message as it would appear on the latest version of FortiClient.

4. Click *Save*.


FortiClient Enterprise Management Server
Dashboard
Endpoints
Quarantine Management
Software Inventory
Endpoint Profiles
Gateway Lists
Administration
System Settings
Server
Logs
FortiGuard
Endpoints
Login Banner
EMS for Chromebooks
EMS Alerts
Endpoint Alerts
SMTP Server
Custom Messages
Help
Name
Description
Endpoint Quarantine Message
Message displayed on endpoints if they are quarantined
Preview
Quarantine
Quarantined by Builtin\admin
Contact your network administrator for details at 555-555-5555.
Enter a one-time access code
The preview might be different from the actual window.
Message
Contact your network administrator for details at 555-555-5555.
63/512
Save
Discard Changes

Creating a Support Package

You can create a support package to provide to the Fortinet technical support team for troubleshooting. Creating a support package backs up your database, but clears all sensitive username and password fields.

To create a support package:

1. Go to *Help* > *Create Support Package*. The *Create Support Package* dialog box displays.
2. In the *Password* box, type your administrative password.
3. In the *Confirm Password* box, type your password again.
4. Click *Create Support Package*.

Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.